

EUROPEAN PATENT OFFICE

Patent Abstracts of Japan

PUBLICATION NUMBER : 09214556
PUBLICATION DATE : 15-08-97

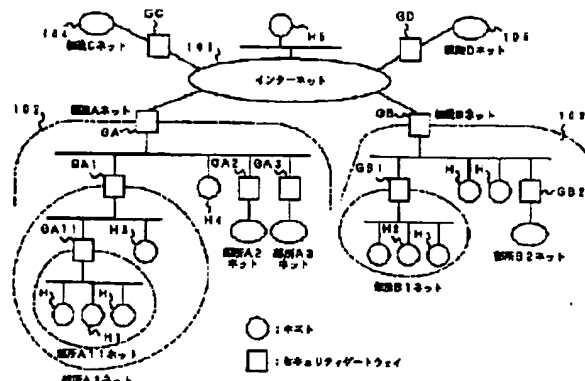
APPLICATION DATE : 07-11-96
APPLICATION NUMBER : 08295116

APPLICANT : TOSHIBA CORP;

INVENTOR : OKAMOTO TOSHIO;

INT.CL. : H04L 12/56 G09C 1/00 G09C 1/00
H04L 9/32

TITLE : PACKET TRANSFER METHOD,
PACKET PROCESSOR, PACKET
CIPHERING METHOD, PACKET
DECODING METHOD AND PACKET
CIPHERING PROCESSING METHOD



ABSTRACT : PROBLEM TO BE SOLVED: To confirm the adequacy of each packet in each packet processing unit by conducting verification processing among packet processing units each managing a transmission source computer and a destination computer.

SOLUTION: Computers H3, H4 are directly contained respectively in management networks A1, A in the computer network. A packet passes security gateway GA while it is reached finally to a destination host from a source host. Each GA executes packet verification processing in the case of transmission of a packet externally or reception of the packet, and a verification key is provided link by link in a form along with a passing path among the GAs. A GA in existence in a packet path transfers packets to its adjacent GA while repeating code resetting due to check/generation of a packet verification code.

COPYRIGHT: (C)1997,JPO

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-214556

(43) 公開日 平成9年(1997)8月15日

(51) Int.Cl. ⁹	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 12/56		9466-5K	H 0 4 L 11/20	1 0 2 A
G 0 9 C 1/00	6 4 0	7259-5 J	G 0 9 C 1/00	6 4 0 A
	6 6 0	7259-5 J		6 6 0 E
H 0 4 L 9/32			H 0 4 L 9/00	6 7 3 B
				6 7 5 A

審査請求 未請求 請求項の数21 O L (全 38 頁)

(21) 出願番号 特願平8-295116

(22) 出願日 平成8年(1996)11月7日

(31) 優先権主張番号 特願平7-312593

(32) 優先日 平7(1995)11月30日

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願平7-313307

(32) 優先日 平7(1995)11月30日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 新保 淳

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72) 発明者 井上 淳

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72) 発明者 石山 政浩

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(74) 代理人 弁理士 鈴江 武彦 (外6名)

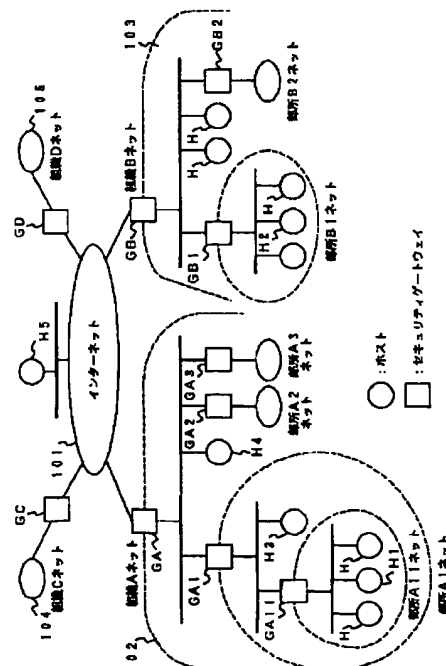
最終頁に続く

(54) 【発明の名称】 パケット転送方法、パケット処理装置、パケット暗号化方法、パケット復号化方法及びパケット暗号処理方法

(57) 【要約】

【課題】 階層化された個々の計算機ネットワークを安全に保護可能なパケット転送方法を提供すること。

【解決手段】 所定管理単位のネットワークとその外部の接続点に通過パケットを認証するパケット管理装置がパケット転送する方法で、送信端末を管理するパケット管理装置は、パケット内のアドレス情報にて少なくとも定まる次段と最終段のパケット管理装置に対する認証鍵を用いて得た2つの認証データをパケットに添付して転送し、パケットを中継するあるいは受信端末を管理するパケット管理装置は、パケット内のアドレス情報にて定まる認証鍵を用いパケット内の自装置対応の認証データの正当性を検査し、検査に通った場合、パケットを次段あるいは受信端末に転送する。



【特許請求の範囲】

【請求項1】所定の管理単位の計算機ネットワークと該計算機ネットワーク外部との接続点に、通過するパケットを認証し、該パケット内のアドレス情報に基づき転送するパケット処理装置を設け、送信元計算機から受信先計算機に至るまでに複数のパケット処理装置を経由してパケットを転送するパケット転送方法であって、

前記送信元計算機を管理するパケット処理装置は、少なくとも、該送信元計算機から受信したパケット内のアドレス情報により定まる、受信先計算機を管理するパケット処理装置に対する認証鍵を用いて、該パケットに対する第1の認証データを求めるとともに、該アドレス情報により定まる、該パケットの次の転送先となるパケット処理装置に対する認証鍵を用いて、該パケットに対する第2の認証データを求め、求められた認証データを該パケットに添付して該次の転送先となるパケット処理装置に転送し、

前記パケットを中継するパケット処理装置は、受信した前記パケット内のアドレス情報により定まる認証鍵を用いて、該パケットに添付された自装置に対応する認証データの正当性を検査し、検査に通った場合、該パケットをそのまま又は所定の処理を施した後に、次の転送先となるパケット処理装置に転送し、

前記パケットの受信先となる計算機を管理するパケット処理装置は、少なくとも、受信したパケット内のアドレス情報により定まる、送信元計算機を管理するパケット処理装置に対応する認証鍵を用いて、該パケット内に添付された自装置に対応する認証データの正当性を検査し、検査に通った場合、該パケットを受信先計算機に転送することを特徴とするパケット転送方法。

【請求項2】前記パケットを中継するパケット処理装置は、受信した前記パケット内のアドレス情報により定まる認証鍵を用いて、該パケットに添付された自装置に対応する認証データの正当性を検査し、検査に通った場合、前記アドレス情報により定まる、次の転送先となるパケット処理装置に対する認証鍵を用いて、該パケットに対する新たな第2の認証データを求め、この新たな第2の認証データを該パケットに添付して該次の転送先となるパケット処理装置に転送することを特徴とする請求項1に記載のパケット転送方法。

【請求項3】前記送信元計算機を管理するパケット処理装置は、該送信元計算機から受信したパケット内のアドレス情報により定まる、受信先計算機を管理するパケット処理装置に対する認証鍵を用いて、該パケットに対する第1の認証データを求めるとともに、該アドレス情報により定まる、該パケットの転送経路上に存在する他のパケット処理装置に対応に設けられた認証鍵を用いて、該パケットに対する第2の認証データを該認証鍵ごとに求め、第1の認証データおよび各認証鍵に対応する第2の認証データを該パケットに添付して該次の転送先となる

パケット処理装置に転送することを特徴とする請求項1に記載のパケット転送方法。

【請求項4】前記送信元計算機を管理するパケット処理装置は、該送信元計算機から受信したパケット内のアドレス情報により定まる、受信先計算機を管理するパケット処理装置に対する認証鍵を用いて、該パケットに対する第1の認証データを求めるとともに、該アドレス情報により定まる、転送経路上に存在する他のパケット処理装置に共通の認証鍵を用いて、該パケットに対する第2の認証データを求め、第1の認証データおよび第2の認証データを該パケットに添付して該次の転送先となるパケット処理装置に転送することを特徴とする請求項1に記載のパケット処理装置。

【請求項5】所定の管理単位の計算機ネットワークと該計算機ネットワーク外部との接続点に、通過するパケットを認証し、該パケット内のアドレス情報に基づき転送するパケット処理装置を設け、送信元計算機から受信先計算機に至るまでに複数のパケット処理装置を経由してパケットを転送するパケット転送方法であって、

前記送信元計算機を管理するパケット処理装置は、該送信元計算機から受信したパケット内のアドレス情報により定まる、受信先計算機を管理するパケット処理装置に対応する認証鍵を用いて、該パケットに対する認証データを求め、求められた認証データを該パケットに添付して次段のパケット処理装置に転送し、

前記パケットを中継するパケット処理装置は、受信した前記パケットが前段のパケット処理装置から転送されたものであれば次段のパケット処理装置に転送し、

前記パケットの受信先となる計算機を管理するパケット処理装置は、前記パケット内のアドレス情報により定まる認証鍵を用いて、該パケットに添付された認証データの正当性を検査し、検査に通った場合、該パケットを受信先計算機に転送することを特徴とするパケット転送方法。

【請求項6】前記送信元計算機または前記受信先計算機が、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機である場合に、前記送信元計算機を管理するパケット処理装置または前記受信先計算機を管理するパケット処理装置の機能を前記送信元計算機内または前記受信先計算機内で実現することを特徴とする請求項1ないし5のいずれか1項に記載のパケット転送方法。

【請求項7】前記送信元計算機が、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機であって、該移動計算機が本来接続されているネットワークを離れて他のネットワークに接続され、受信先計算機と通信を行う場合、

前記移動計算機は、少なくとも、受信先計算機を管理するパケット処理装置に対する認証鍵を用いて、該パケットに対する第1の認証データを求めるとともに、最初に

パケットを通過させるパケット処理装置に対する認証鍵を用いて、該パケットに対する第2の認証データを求め、求められた認証データを該パケットに添付して送出することを特徴とする請求項1ないし5のいずれか1項に記載のパケット転送方法。

【請求項8】前記第1の認証データは、送信元計算機が発信した送信パケットの全てのビットに依存した認証データとし、前記第2の認証データは、元の送信パケットと前記第1の認証データを合わせたデータのうち、前記第1の認証データを含む所定の一部のビットに依存した認証データとすることを特徴とする請求項1ないし7のいずれか1項に記載のパケット転送方法。

【請求項9】前記第1の認証データおよび前記第2の認証データはいずれも、送信元計算機が発信した送信パケットの全てのビットに依存した認証データとすることを特徴とする請求項1ないし7のいずれか1項に記載のパケット転送方法。

【請求項10】所定の管理単位の計算機ネットワークと該計算機ネットワーク外部との接続点に設けられ、自装置が管理する送信元計算機から複数のパケット処理装置を介した先に存在する受信先計算機に向けてパケットを転送するパケット処理装置であって、少なくとも、受信先計算機を管理するパケット処理装置に対する第1の認証鍵および次の転送先となるパケット処理装置に対する第2の認証鍵をパケット内のアドレス情報に対応付けて記憶する認証鍵記憶手段と、受信した前記パケット内のアドレス情報により定まる前記認証鍵を夫々用いて、該パケットに対する認証データを該認証鍵ごとに生成する認証データ生成手段と、前記認証データ生成手段により生成された認証データを該パケットに添付するパケット整形手段と、前記アドレス情報に基づき前記パケット整形手段により認証データの添付されたパケットを次段のパケット処理装置に転送する転送手段とを具備したことを特徴とするパケット処理装置。

【請求項11】前記認証鍵記憶手段には、転送経路上に存在するパケット処理装置対応に設けられた認証鍵群をパケット内のアドレス情報に対応付けて記憶することを特徴とする請求項10に記載のパケット処理装置。

【請求項12】所定の管理単位の計算機ネットワークと該計算機ネットワーク外部との接続点に設けられ、パケットを中継するパケット処理装置であって、前段のパケット処理装置に対応する第1の認証鍵および後段のパケット処理装置に対応する第2の認証鍵をパケット内のアドレス情報に対応付けて記憶する認証鍵記憶手段と、受信した前記パケット内のアドレス情報により定まる前記第1の認証鍵を用いて、前段のパケット処理装置により該パケットに添付された認証データの正当性を検査する認証データ検査手段と、

前記認証データ検査手段により正当性が確認された場合に、前記アドレス情報により定まる前記第2の認証鍵を用いて新たに生成された認証データを該パケットに添付するパケット整形手段と、

前記アドレス情報に基づき前記パケット整形手段により認証データの添付されたパケットを次段のパケット処理装置に転送する転送手段とを具備したことを特徴とするパケット処理装置。

【請求項13】所定の管理単位の計算機ネットワークと該計算機ネットワーク外部との接続点に設けられるパケット処理装置にて外部方向に通信されるパケットを暗号化するパケット暗号化方法において、予め格納された、他のパケット処理装置を介さずに直接管理する計算機群のアドレス情報と、通過するパケット内に書き込まれている送信元計算機のアドレス情報とを比較し、該パケットの送信元が直接管理する計算機であるか否かを判断し、

前記パケットの送信元が直接管理する計算機であると判断された場合に、該パケット内のデータ本体の部分を暗号化することを特徴とするパケット暗号化方法。

【請求項14】所定の管理単位の計算機ネットワークと該計算機ネットワーク外部との接続点に設けられるパケット処理装置にて外部方向に通信されるパケットを暗号化するパケット暗号化方法において、通過するパケット内に書き込まれている暗号化完了または暗号化未完了を示す暗号化情報の内容および署名情報の有無を調べ、

暗号化未完了であり、かつ、署名情報が存在しない場合、前記パケット内のデータ本体の部分を暗号化するとともに、該パケットに対して、前記暗号化情報を暗号化完了を示す内容にし、および暗号化を行った自装置の署名情報を付加することを特徴とするパケット暗号化方法。

【請求項15】前記パケット内に書き込まれている暗号化完了または暗号化未完了を示す暗号化情報の内容および署名情報の有無を調べた結果、暗号化完了でありかつ署名情報が存在しない場合または暗号化未完了でありかつ署名情報が存在する場合は、エラーを通知するように制御することを特徴とする請求項14に記載のパケット暗号化方法。

【請求項16】所定の管理単位の計算機ネットワークと該計算機ネットワーク外部との接続点に設けられるパケット処理装置にて外部方向に通信されるパケットを暗号化するパケット暗号化方法において、通過するパケット内に書き込まれている暗号化完了または暗号化未完了を示す暗号化情報の内容および署名情報の有無を調べ、

暗号化未完了であり、かつ、署名情報が存在しない場合、予め格納された、自装置の設置箇所から末端の計算機に至る下位ネットワークに接続されている計算機のア

ドレス情報と、各計算機に至るネットワーク経路内に設置されたパケット処理装置の数の情報との対応情報をもとに、前記パケット内に書き込まれている送信元計算機のアドレス情報から、対応するパケット処理装置の数の情報を求め、

求められたパケット処理装置の数の情報と、前記パケット内に書き込まれている暗号化レベル情報とが等しい場合、前記パケット内のデータ本体の部分を暗号化するとともに、該パケットに対して、前記暗号化情報を暗号化完了を示す内容にし、および暗号化を行った自装置の署名情報を付加することを特徴とするパケット暗号化方法。

【請求項17】前記パケット内に書き込まれている暗号化完了または暗号化未完了を示す暗号化情報の内容、署名情報の有無、および暗号化レベル情報の内容の間に矛盾が存在する場合は、エラーを通知するように制御することを特徴とする請求項16に記載のパケット暗号化方法。

【請求項18】所定の管理単位の計算機ネットワークと該計算機ネットワーク外部との接続点に設けられるパケット処理装置にて外部方向から通信されるパケットを復号化するパケット復号化方法において、予め格納された、他のパケット処理装置を介さずに直接管理する計算機群のアドレス情報と、通過するパケット内に書き込まれている受信先計算機のアドレス情報とを比較し、該パケットの転送先が直接管理する計算機であるかを判断し、

前記パケットの転送先が直接管理する計算機であると判断された場合に、該パケット内のデータ本体の部分を復号化することを特徴とするパケット復号化方法。

【請求項19】所定の管理単位の計算機ネットワークと該計算機ネットワーク外部との接続点に設けられるパケット処理装置にて外部方向から通信されるパケットを復号化するパケット復号化方法において、通過するパケット内に書き込まれている暗号化完了または暗号化未完了を示す暗号化情報の内容および署名情報の有無を調べ、

暗号化完了であり、かつ、署名情報が存在する場合、予め格納された、自装置の設置箇所から末端の計算機に至る下位ネットワークに接続されている計算機のアドレス情報と、各計算機に至るネットワーク経路内に設置されたパケット処理装置の数の情報との対応情報をもとに、前記パケット内に書き込まれている受信先計算機のアドレス情報から、対応するパケット処理装置の数の情報を求め、

求められたパケット処理装置の数の情報と、前記パケット内に書き込まれている復号化レベル情報とが等しい場合、前記パケット内のデータ本体の部分を復号化することを特徴とするパケット復号化方法。

【請求項20】前記復号化レベル情報を、前記パケット

の送信元計算機が暗号化を行なう処理装置を指定するための前記暗号化レベル情報と共通化したことを特徴とする請求項19に記載のパケット復号化方法。

【請求項21】前記計算機が、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機であって、該移動計算機が本来接続されているネットワークを離れて他のネットワークに接続され、他の計算機と通信を行う場合、

該移動計算機は、自装置が送信元となる計算機であるとき、自装置内で該パケット内のデータ本体の部分を暗号化して送出し、

自装置が受信先となる計算機であるとき、自装置内で該パケット内のデータ本体の部分を復号化することを特徴とする請求項13ないし20のいずれか1項に記載のパケット暗号処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、移動計算機を含む複数の計算機間でオープンなネットワークを介してデータ通信を行なう場合に、受信したパケットが正当な計算機もしくは利用者からのものであるかどうかを認証し、正当なパケットのみを転送制御し、さらには組織外部へのデータ転送にあたり外部への情報漏洩を防ぐためパケットの暗号化を行う、パケット転送方法、パケット処理装置、パケット暗号化方法、パケット復号化方法及びパケット暗号処理方法に関する。

【0002】

【従来の技術】インターネットの普及により、遠隔地の計算機にログインしたり、遠隔地の計算機に対しファイルを転送したりすることが可能となっている。電子メールやworld wide web (WWW)などのサービスも利用できる。その一方、インターネットではセキュリティを考慮したプロトコルやシステムの構築が遅れてきたため、悪意の利用者が遠隔ネットワークの計算機に侵入して機密情報を盗んだり、重要なファイルを消去したり、さらには外部への通信情報が盗聴されるといった不正行為が行われる可能性があった。

【0003】このような不正行為に対抗するため、企業などのネットワークにはファイアウォール、もしくはセキュリティゲートウェイと呼ばれるシステムが構築される場合が多い。ファイアウォールは企業のローカルなネットワークと広域なインターネットの接続点に設けられ、外部からの不正な侵入や情報漏洩を防止するために通信のフィルタリング（通信の遮断・通過の制御）を実現するシステムである。

【0004】ファイアウォールが危険な外部からの通信を遮断するので、内部のネットワーク（内部ネット）に接続された計算機（ホスト）には特別にセキュリティを強化するための仕組みを講じなくても済むという利点がある。

【0005】ファイアウォールの基本手法に、パケットフィルタがある。パケットフィルタは通信パケットに添付されている送信元ホストと受信元ホストのアドレスと利用サービス（遠隔ログイン（telnet）、ファイル転送（ftp）、電子メール（SMTP）、電子ニュース（NNTP）、WWWサービス（httpなど）に対応するポート番号を基に許可された通信かどうかを判定し、許可されている通信のパケットのみをリレーする手法である。この手法ではパケット内のホスト・アドレスとサービス（ポート番号）を改変困難と仮定すれば十分なセキュリティ機能を提供するが、実際には送信ホストのアドレスを偽ってパケットを送出することは可能である。このような不正行為に対抗するために、暗号を利用した認証機能を用いてパケットのフィルタリングを実施するシステムがある。

【0006】暗号によるパケット認証には一般にMAC（Message Authentication Code）と呼ばれる手法が用いられる。これは、パケットの送信側と受信側が秘密の鍵情報を共有していることを前提とする。送信側は各パケットごとに、そのデータの全ビットと鍵Kに依存したダイジェスト情報を計算し、パケットに添付する。すなわち、 $MAC = f(K, data)$ を計算する。ここでfはMAC計算アルゴリズム、dataはパケットの内容を表す。一方、パケットの受信側は受け取ったパケットの内容と鍵Kから送信側と同じ計算を行い、計算したMACの値とパケットに添付されたMACが一致する場合には、送信者とパケット内容が送信データそのものであることを認証する。

【0007】ファイアウォールにMACによる認証機能を導入することは、例えば文献J. Ioannidis and M. Blaze, "The Architecture and Implementation of Network-Layer Security under Unix," USENIX/4th UNIX Security symposium, pp. 29-39 (1993) に示されている。

【0008】このようにすると、パケット中のアドレスやポート番号を偽った送信や伝送中のパケットの改ざんは検出できるため、ファイアウォールシステムの安全性が飛躍的に向上する。これを認証機能付きファイアウォールと呼ぶことにする。

【0009】しかし、従来の認証機能付きファイアウォールが対象としているのは、保護すべきネットワークが1階層の場合に限定されていた。すなわち、送信ホストもしくは送信ホストを収容するネットワークのファイアウォールがMACをパケットに添付し、受信ホストを収容するネットワークのファイアウォールをMACを検査する仕組みである。保護ネットワークが階層的になった場合には十分に対応できない。なぜなら受信側の保護ネットワークが2階層の場合、送信ホスト側のファイア

ウォールと受信側第1階層のファイアウォールは鍵Kを共有するため、MACを検査することはできるが、受信側第2階層のファイアウォールは鍵Kを持たないので同じパケットを受け取ってもMAC検査ができないからである。

【0010】仮に受信側第1階層のファイアウォール、受信側第2階層のファイアウォール、送信側ファイアウォールが鍵Kを共有することになると、受信側第1階層のファイアウォールから送信側ファイアウォールになりすまして受信側第2階層ファイアウォールへパケットを送り込むことができる。

【0011】最近では携帯型計算機を利用する場面も多くなっており、多部署のネットワークに携帯計算機を接続して、その移動計算機が本来所属しているネットワークのサーバ計算機や移動先の計算機などと通信する場面も増加している。このような場合でも従来の認証機能付きファイアウォールの機能では限界がある。すなわち、認証機能付きファイアウォールでは、訪問先のネットワークのファイアウォールと通信相手のネットワークのファイアウォールの間でパケットの検査は行えるが、移動計算機と訪問先のファイアウォールとの認証や移動計算機と通信先のファイアウォールとの認証をどのようにして一貫して行うかは未解決のままである。

【0012】以上の説明した認証の問題以外に、通信パケット内容の保護という問題もある。すなわち、特に機密性の高いデータを外部ネットワークを介して通信する状況では、外部にデータパケットを送出する前にその内容を暗号化し、受信したサイトで復号化するという方法がある。この方法も保護すべきネットワークが1階層の場合にはパケットの方向性のみを暗号化・復号化の判定に利用すれば良いが、保護すべきネットワークが階層された場合や、移動計算機を利用したモバイル・コンピューティング環境では、暗号化・復号化の制御をどのマシンで、どのような判断基準で行うかという問題がある。特に、パケットを階層間に亘って転送する場合に各階層での復号・再暗号化の繰り返しの処理効率の低下を回避しつつ安全性を確保することは困難であった。また、暗号通信すべき領域と平文で通信すべき領域を柔軟に制御しつつ安全性を確保することは困難であった。

【0013】

【発明が解決しようとする課題】 以上のように、従来のシステムでは、保護すべきネットワークが階層化された計算機ネットワーク等では、各階層のネットワークを安全に保護することは困難であった。また、暗号通信を効率的かつ安全に行うことは困難であった。

【0014】本発明は、上記事情を考慮してなされたものであり、保護すべき計算機ネットワークが階層化された場合や移動計算機をサポートするモバイル・コンピューティング環境においても、個々のネットワークを安全に保護可能なパケット転送方法及びパケット処理装置を

提供することを目的とする。

【0015】また、本発明は、保護すべき計算機ネットワークが階層化された場合や移動計算機をサポートするモバイル・コンピューティング環境においても、通信されるデータ内容を効率的かつ安全に保護可能なパケット暗号化方法、パケット復号化方法及びパケット暗号処理方法を提供することを目的とする。

【0016】

【課題を解決するための手段】本発明（請求項1）は、所定の管理単位の計算機ネットワークと該計算機ネットワーク外部との接続点に、通過するパケットを認証し、該パケット内のアドレス情報に基づき転送するパケット処理装置（例えば、セキュリティゲートウェイ）を設け、送信元計算機から受信先計算機に至るまでに複数のパケット処理装置を経由してパケットを転送するパケット転送方法であって、前記送信元計算機を管理するパケット処理装置は、少なくとも、該送信元計算機から受信したパケット内のアドレス情報により定まる、受信先計算機を管理するパケット処理装置に対する認証鍵（証明用認証鍵）を用いて、該パケットに対する第1の認証データを求めるとともに、該アドレス情報により定まる、該パケットの次の転送先となるパケット処理装置に対する認証鍵（証明用認証鍵）を用いて、該パケットに対する第2の認証データを求め、求められた認証データを該パケットに添付して該次の転送先となるパケット処理装置に転送し、前記パケットを中継するパケット処理装置は、受信した前記パケット内のアドレス情報により定まる認証鍵（証明用認証鍵）を用いて、該パケットに添付された自装置に対応する認証データの正当性を検査し、検査に通った場合、該パケットをそのまま又は所定の処理を施した後に、次の転送先となるパケット処理装置に転送し、前記パケットの受信先となる計算機を管理するパケット処理装置は、少なくとも、受信したパケット内のアドレス情報により定まる、送信元計算機を管理するパケット処理装置に対応する認証鍵（検査用認証鍵）を用いて、該パケット内に添付された自装置に対応する認証データの正当性を検査し、検査に通った場合、該パケットを受信先計算機に転送することを特徴とする。

【0017】本発明によれば、前記パケットを中継するパケット処理装置は、自装置に対応する認証データの正当性を検査するので、パケットが経路に沿って隣のパケット処理装置から転送されていること、内容に改ざんがないことを確認できる。また、受信先計算機を管理するパケット処理装置は、少なくとも、送信元計算機を管理するパケット処理装置により添付された認証データを検査するので、パケットが送信元を管理するパケット処理装置により発信されたものであること、内容に改ざんがないことを確認できる。

【0018】本発明（請求項2）は、請求項1に記載のパケット転送方法において、前記パケットを中継するパ

ケット処理装置は、受信した前記パケット内のアドレス情報により定まる認証鍵（証明用認証鍵）を用いて、該パケットに添付された自装置に対応する認証データの正当性を検査し、検査に通った場合、前記アドレス情報により定まる、次の転送先となるパケット処理装置に対する認証鍵（証明用認証鍵）を用いて、該パケットに対する新たな第2の認証データを求め、この新たな第2の認証データを該パケットに添付して該次の転送先となるパケット処理装置に転送することを特徴とする。

【0019】前記パケットの受信先となる計算機を管理するパケット処理装置は、受信したパケット内のアドレス情報により定まる、送信元計算機を管理するパケット処理装置に対応する認証鍵（検査用認証鍵）を用いて、該パケット内に添付された自装置に対応する第1の認証データの正当性を検査し、その検査に通った場合、該パケットを受信先計算機に転送する。

【0020】あるいは、前記パケットの受信先となる計算機を管理するパケット処理装置は、受信したパケット内のアドレス情報により定まる、送信元計算機を管理するパケット処理装置に対応する認証鍵（検査用認証鍵）と、前段のパケット処理装置に対応する認証鍵（検査用認証鍵）を夫々用いて、該パケット内に添付された自装置に対応する第1の認証データと第2の認証データの正当性を検査し、両方の検査に通った場合、該パケットを受信先計算機に転送する。

【0021】本発明によれば、パケット転送経路上に存在してパケットを中継するパケット処理装置では、隣のパケット処理装置との間で第2の認証データの検査・生成を繰り返しながら、パケットの転送が行われる。これにより、各パケット処理装置は、パケットが経路に沿って隣のパケット処理装置から転送されていること、内容に改ざんがないことを確認できる。また、受信先計算機を管理するパケット処理装置は、少なくとも、送信元計算機を管理するパケット処理装置により添付された第1の認証データをも検査する。この認証データの検査によりパケットが送信元を管理するパケット処理装置により発信されたものであること、内容に改ざんがないことを確認できる。さらに、受信先計算機を管理するパケット処理装置は、隣のパケット処理装置との間での第2の認証データの検査を行うようにした場合、パケットが経路に沿って隣のパケット処理装置から転送されていること、内容に改ざんがないことをも確認できる。

【0022】本発明（請求項3）は、請求項1に記載のパケット転送方法において、前記送信元計算機を管理するパケット処理装置は、該送信元計算機から受信したパケット内のアドレス情報により定まる、受信先計算機を管理するパケット処理装置に対する認証鍵（証明用認証鍵）を用いて、該パケットに対する第1の認証データを求めるとともに、該アドレス情報により定まる、該パケットの転送経路上に存在する他のパケット処理装置対応

に設けられた認証鍵（証明用認証鍵）を用いて、該パケットに対する第2の認証データを該認証鍵ごとに求め、第1の認証データおよび各認証鍵に対応する第2の認証データを該パケットに添付して該次の転送先となるパケット処理装置に転送することを特徴とする。

【0023】前記パケットの受信先となる計算機を管理するパケット処理装置は、受信したパケット内のアドレス情報により定まる、送信元計算機を管理するパケット処理装置に対応する認証鍵（検査用認証鍵）を用いて、該パケット内に添付された第1の認証データの正当性を検査し、検査に通った場合、該パケットを受信先計算機に転送することになる。

【0024】本発明によれば、パケット転送経路上に存在するパケット処理装置では、自装置に対応する認証コードの検査を行い、検査に通ればパケットを転送する。これにより、パケットが送信元計算機を管理するパケット処理装置により発信されたものであること、内容に改ざんがないことを各経路上のパケット処理装置が確認できる。

【0025】本発明（請求項4）は、請求項1に記載のパケット処理装置において、前記送信元計算機を管理するパケット処理装置は、該送信元計算機から受信したパケット内のアドレス情報により定まる、受信先計算機を管理するパケット処理装置に対する認証鍵（証明用認証鍵）を用いて、該パケットに対する第1の認証データ（受信用認証コード）を求めるとともに、該アドレス情報により定まる、転送経路上に存在する他のパケット処理装置に共通の認証鍵（証明用認証鍵）を用いて、該パケットに対する第2の認証データ（通過用認証コード）を求め、第1の認証データおよび第2の認証データを該パケットに添付して該次の転送先となるパケット処理装置に転送することを特徴とする。

【0026】前記パケットを中継するパケット処理装置は、受信したパケット内のアドレス情報により定まる認証鍵（検査用認証鍵）を用いて、該パケット内に添付された第2の認証データ（通過用認証コード）の正当性を検査することになる。

【0027】また、前記パケットの受信先となる計算機を管理するパケット処理装置は、受信したパケット内のアドレス情報により定まる、送信元計算機を管理するパケット処理装置に対応する認証鍵（検査用認証鍵）を用いて、該パケット内に添付された第1の認証データ（受信用認証コード）の正当性を検査し、検査に通った場合、該パケットを受信先計算機に転送することになる。

【0028】本発明によれば、パケットの経路上に存在するパケット処理装置は、自装置に対応する認証コードの検査を行い、検査に通ればパケットを転送する。これにより、パケットが送信元計算機を管理するパケット処理装置により発信されたものであること、内容に改ざんがないことを各経路上のパケット処理装置が確認できる。

【0029】本発明（請求項5）は、所定の管理単位の計算機ネットワークと該計算機ネットワーク外部との接続点に、通過するパケットを認証し、該パケット内のアドレス情報に基づき転送するパケット処理装置（例えば、セキュリティゲートウェイ）を設け、送信元計算機から受信先計算機に至るまでに複数のパケット処理装置を経由してパケットを転送するパケット転送方法であって、前記送信元計算機を管理するパケット処理装置は、該送信元計算機から受信したパケット内のアドレス情報により定まる、受信先計算機を管理するパケット処理装置に対応する認証鍵（証明用認証鍵）を用いて、該パケットに対する認証データを求め、求められた認証データを該パケットに添付して次段のパケット処理装置に転送し、前記パケットを中継するパケット処理装置は、受信した前記パケットが前段のパケット処理装置から転送されたものであれば次段のパケット処理装置に転送し、前記パケットの受信先となる計算機を管理するパケット処理装置は、前記パケット内のアドレス情報により定まる認証鍵（検査用認証鍵）を用いて、該パケットに添付された認証データの正当性を検査し、検査に通った場合、該パケットを受信先計算機に転送することを特徴とする。

【0030】本発明によれば、パケットの経路上に存在するパケット処理装置は、パケットが前段のパケット処理装置から転送されたものであり、さらに転送先が次段のパケット処理装置であれば、パケットを転送する。また、受信先計算機を管理するパケット処理装置は、自装置に対応する認証コードの検査を行い、検査に通ればパケットを転送する。これにより、パケットが送信元計算機を管理するパケット処理装置により発信されたものであること、内容に改ざんがないことを確認できる。

【0031】本発明（請求項6）は、請求項1ないし5のいずれか1項に記載のパケット転送方法において、前記送信元計算機または前記受信先計算機が、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機である場合に、前記送信元計算機を管理するパケット処理装置または前記受信先計算機を管理するパケット処理装置の機能を前記送信元計算機内または前記受信先計算機内で実現することを特徴とする。

【0032】本発明（請求項7）は、請求項1ないし5のいずれか1項に記載のパケット転送方法において、前記送信元計算機が、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機であって、該移動計算機が本来接続されているネットワークを離れて他のネットワークに接続され、受信先計算機と通信を行う場合、前記移動計算機は、少なくとも、受信先計算機を管理するパケット処理装置に対する認証鍵（証明用認証鍵）を用いて、該パケットに対する第1の認証データを求めるとともに、最初にパケットを通過させるパケット処理装置に対する認証鍵（証明用認証鍵）を用い

て、該パケットに対する第2の認証データを求め、求められた認証データを該パケットに添付して送出することを特徴とする。

【0033】本発明（請求項8）は、請求項1ないし7のいずれか1項に記載のパケット転送方法において、前記第1の認証データは、送信元計算機が発信した送信パケットの全てのビットに依存した認証データとし、前記第2の認証データは、元の送信パケットと前記第1の認証データを合わせたデータのうち、前記第1の認証データを含む所定の一部のビットに依存した認証データとすることを特徴とする。

【0034】本発明によれば、第2の認証データの生成・検査を効率化することができる。

【0035】本発明（請求項9）は、請求項1ないし7のいずれか1項に記載のパケット転送方法において、前記第1の認証データおよび前記第2の認証データはいずれも、送信元計算機が発信した送信パケットの全てのビットに依存した認証データとすることを特徴とする。

【0036】本発明（請求項10）は、所定の管理単位の計算機ネットワークと該計算機ネットワーク外部との接続点に設けられ、自装置が管理する送信元計算機から複数のパケット処理装置（例えば、セキュリティゲートウェイ）を介した先に存在する受信先計算機に向けてパケットを転送するパケット処理装置であって、少なくとも、受信先計算機を管理するパケット処理装置に対する第1の認証鍵（証明用認証鍵）および次の転送先となるパケット処理装置に対する第2の認証鍵（証明用認証鍵）をパケット内のアドレス情報に対応付けて記憶する認証鍵記憶手段と、受信した前記パケット内のアドレス情報により定まる前記認証鍵を夫々用いて、該パケットに対する認証データを該認証鍵ごとに生成する認証データ生成手段と、前記認証データ生成手段により生成された認証データを該パケットに添付するパケット整形手段と、前記アドレス情報に基づき前記パケット整形手段により認証データの添付されたパケットを次段のパケット処理装置に転送する転送手段とを具備したことを特徴とする。

【0037】本発明（請求項11）は、請求項10に記載のパケット処理装置において、前記認証鍵記憶手段には、転送経路上に存在するパケット処理装置対応に設けられた認証鍵（証明用認証鍵）群をパケット内のアドレス情報に対応付けて記憶することを特徴とする。

【0038】本発明によれば、パケットの経路に存在するパケット処理装置は、転送に先だって、自装置に対応する認証コードの検査を行うことができる。これにより、パケットが送信元計算機を管理するパケット処理装置により発信されたものであること、内容に改ざんがないことを各経路上のパケット処理装置が確認できる。

【0039】本発明（請求項12）は、所定の管理単位の計算機ネットワークと該計算機ネットワーク外部との

接続点に設けられ、パケットを中継するパケット処理装置（例えば、セキュリティゲートウェイ）であって、前段のパケット処理装置に対応する第1の認証鍵（検査用認証鍵）および後段のパケット処理装置に対応する第2の認証鍵（証明用認証鍵）をパケット内のアドレス情報に対応付けて記憶する認証鍵記憶手段と、受信した前記パケット内のアドレス情報により定まる前記第1の認証鍵を用いて、前段のパケット処理装置により該パケットに添付された認証データの正当性を検査する認証データ検査手段と、前記認証データ検査手段により正当性が確認された場合に、前記アドレス情報により定まる前記第2の認証鍵を用いて新たに生成された認証データを該パケットに添付するパケット整形手段と、前記アドレス情報に基づき前記パケット整形手段により認証データの添付されたパケットを次段のパケット処理装置に転送する転送手段とを具備したことを特徴とする。

【0040】本発明によれば、パケット経路の間に存在してパケットを中継するパケット処理装置では、隣のパケット処理装置との間でパケット認証データの検査・生成を繰り返しながら、パケットの転送が行われる。これにより、各パケット処理装置は、パケットが経路に沿って隣のパケット処理装置から転送されていること、内容に改ざんがないことを確認できる。

【0041】以上の各発明において、好ましくは、送信元計算機を管理するパケット処理装置は、送信元計算機自体に組み込まれたものであっても良いし、送信元計算機を他のパケット処理装置を介さずに直接管理するパケット処理装置でも良い。

【0042】同様に、好ましくは、受信先計算機を管理するパケット処理装置は、受信先計算機自体に組み込まれたものであっても良いし、受信先計算機を他のパケット処理装置を介さずに直接管理するパケット処理装置でも良い。

【0043】また、好ましくは、各パケット処理装置に対応する認証データは、その都度、各パケット処理装置にて転送に先だってパケットから除去しても良いし、受信先となる計算機を管理するパケット処理装置にて、まとめて除去しても良い。

【0044】本発明（請求項13）は、所定の管理単位の計算機ネットワークと該計算機ネットワーク外部との接続点に設けられるパケット処理装置（例えば、セキュリティゲートウェイ）にて外部方向に通信されるパケットを暗号化するパケット暗号化方法において、予め格納された、他のパケット処理装置を介さずに直接管理する計算機群のアドレス情報と、通過するパケット内に書き込まれている送信元計算機のアドレス情報とを比較し、該パケットの送信元が直接管理する計算機であるか否かを判断し、前記パケットの送信元が直接管理する計算機であると判断された場合に、該パケット内のデータ本体の部分を暗号化することを特徴とする。

【0045】本発明によれば、重要な情報をネットワークを介して通信する際に、送信元計算機を直接管理するパケット処理装置だけがパケットを暗号化するので、転送にあたってパケットを暗号化する処理を1回のみ行うようにすることができ、暗号化の処理に起因するデータ転送効率の低下を防止することができる。

【0046】本発明（請求項14）は、所定の管理単位の計算機ネットワークと該計算機ネットワーク外部との接続点に設けられるパケット処理装置（例えば、セキュリティゲートウェイ）にて外部方向に通信されるパケットを暗号化するパケット暗号化方法において、通過するパケット内に書き込まれている暗号化完了または暗号化未完了を示す暗号化情報の内容および署名情報の有無を調べ、暗号化未完了であり、かつ、署名情報が存在しない場合、前記パケット内のデータ本体の部分を暗号化するとともに、該パケットに対して、前記暗号化情報を暗号化完了を示す内容にし、および暗号化を行った自装置の署名情報を付加することを特徴とする。

【0047】本発明によれば、重要な情報をネットワークを介して通信する際に、送信元計算機を直接管理するパケット処理装置だけがパケットを暗号化するので、転送にあたってパケットを暗号化する処理を1回のみ行うようにすることができ、暗号化の処理に起因するデータ転送効率の低下を防止することができる。

【0048】本発明（請求項15）は、請求項14に記載のパケット暗号化方法において、前記パケット内に書き込まれている暗号化完了または暗号化未完了を示す暗号化情報の内容および署名情報の有無を調べた結果、暗号化完了でありかつ署名情報が存在しない場合または暗号化未完了でありかつ署名情報が存在する場合は、エラーを通知するように制御することを特徴とする。

【0049】本発明（請求項16）は、所定の管理単位の計算機ネットワークと該計算機ネットワーク外部との接続点に設けられるパケット処理装置（例えば、セキュリティゲートウェイ）にて外部方向に通信されるパケットを暗号化するパケット暗号化方法において、通過するパケット内に書き込まれている暗号化完了または暗号化未完了を示す暗号化情報の内容および署名情報の有無を調べ、暗号化未完了であり、かつ、署名情報が存在しない場合、予め格納された、自装置の設置箇所から末端の計算機に至る下位ネットワークに接続されている計算機のアドレス情報と、各計算機に至るネットワーク経路内に設置されたパケット処理装置の数の情報との対応情報をもとに、前記パケット内に書き込まれている送信元計算機のアドレス情報から、対応するパケット処理装置の数の情報を求め、求められたパケット処理装置の数の情報と、前記パケット内に書き込まれている暗号化レベル情報とが等しい場合、前記パケット内のデータ本体の部分を暗号化するとともに、該パケットに対して、前記暗号化情報を暗号化完了を示す内容にし、および暗号化を

行った自装置の署名情報を付加することを特徴とする。

【0050】本発明によれば、重要な情報をネットワークを介して通信する際に、送信側でパケットを暗号化する処理をユーザの指定する箇所のパケット処理装置で1回のみ行うようにすることができ、暗号化の処理に起因するデータ転送効率の低下を防止することができる。

【0051】本発明（請求項17）は、請求項16に記載のパケット暗号化方法において、前記パケット内に書き込まれている暗号化完了または暗号化未完了を示す暗号化情報の内容、署名情報の有無、および暗号化レベル情報の内容の間に矛盾が存在する場合は、エラーを通知するように制御することを特徴とする。

【0052】本発明（請求項18）は、所定の管理単位の計算機ネットワークと該計算機ネットワーク外部との接続点に設けられるパケット処理装置（例えば、セキュリティゲートウェイ）にて外部方向から通信されるパケットを復号化するパケット復号化方法において、予め格納された、他のパケット処理装置を介さずに直接管理する計算機群のアドレス情報と、通過するパケット内に書き込まれている受信先計算機のアドレス情報とを比較し、該パケットの転送先が直接管理する計算機であるかを判断し、前記パケットの転送先が直接管理する計算機であると判断された場合に、該パケット内のデータ本体の部分を復号化することを特徴とする。

【0053】本発明によれば、重要な情報をネットワークを介して通信する際に、受信先計算機を直接管理するパケット処理装置だけがパケットを復号化するので、転送にあたってパケットを復号化する処理を1回のみ行うようにすることができ、復号化の処理に起因するデータ転送効率の低下を防止することができる。

【0054】本発明（請求項19）は、所定の管理単位の計算機ネットワークと該計算機ネットワーク外部との接続点に設けられるパケット処理装置（例えば、セキュリティゲートウェイ）にて外部方向から通信されるパケットを復号化するパケット復号化方法において、通過するパケット内に書き込まれている暗号化完了または暗号化未完了を示す暗号化情報の内容および署名情報の有無を調べ、暗号化完了であり、かつ、署名情報が存在する場合、予め格納された、自装置の設置箇所から末端の計算機に至る下位ネットワークに接続されている計算機のアドレス情報と、各計算機に至るネットワーク経路内に設置されたパケット処理装置の数の情報との対応情報をもとに、前記パケット内に書き込まれている受信先計算機のアドレス情報から、対応するパケット処理装置の数の情報を求め、求められたパケット処理装置の数の情報と、前記パケット内に書き込まれている復号化レベル情報とが等しい場合、前記パケット内のデータ本体の部分を復号化することを特徴とする。

【0055】本発明によれば、重要な情報をネットワークを介して通信する際に、受信側でパケットを暗号化す

る処理をユーザの指定する箇所のパケット処理装置で1回のみ行うようにすることができ、暗号化の処理に起因するデータ転送効率の低下を防止することができる。

【0056】本発明(請求項20)は、請求項19に記載のパケット復号化方法において、前記復号化レベル情報を、前記パケットの送信元計算機が暗号化を行なうパケット処理装置を指定するための前記暗号化レベル情報と共通化したことを特徴とする。

【0057】パケット処理装置による相互接続は、外部ネットワークとの接続のみならず、組織内の小グループ間でも各組織内部の秘密情報の保護のため設置されるようになっていくと考えられ、その場合、末端の計算機から複数のパケット処理装置を通して各組織間の通信や外部ネットワークとの通信を行うようになる。本発明によれば、そのようなネットワーク構成において、データに含まれる情報を共有すべき最小のネットワーク範囲を認識し、必要なネットワーク階層で1回のみ暗号化、復号化を行い、かつ不要な多段階の暗号化を回避するよう制御することが可能になる。

【0058】本発明(請求項21)に係るパケット転送方法は、請求項13ないし20のいずれか1項において、前記計算機が、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機であって、該移動計算機が本来接続されているネットワークを離れて他のネットワークに接続され、他の計算機と通信を行う場合、該移動計算機は、自装置が送信元となる計算機であるとき、自装置内で該パケット内のデータ本体の部分を暗号化して送出し、自装置が受信先となる計算機であるとき、自装置内で該パケット内のデータ本体の部分を復号化することを特徴とする。

【0059】なお、以上の各装置に係る発明は、方法に係る説明としても成立し、各方法に係る発明は、装置に係る説明としても成立する。

【0060】また、上記の発明は、コンピュータに上記の発明に相当する各手順を実行させるためのプログラムあるいはコンピュータを上記の発明に相当する各手段として機能させるためのプログラムを記録した機械読取り可能な媒体としても成立する。

【0061】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【0062】図1は、本発明を適用する計算機ネットワークの一例である。

【0063】セキュリティゲートウェイの保護および管理の対象となるネットワークを管理対象ネットワークと呼ぶ。

【0064】本実施形態においては、各々のセキュリティゲートウェイに対して、管理対象ネットワークとそれ以外である外部ネットワークが定義され、セキュリティゲートウェイは、外部ネットワークから管理ネットワー

クへの不審なパケットの侵入を防止し、さらには管理ネットワークから外部ネットワークへの不審なパケットの流出を防止する。例えば図1の計算機ネットワークでは、セキュリティゲートウェイGA1の管理ネットワークは部所A1ネットワークであり、セキュリティゲートウェイGA11の管理ネットワークは部所A11ネットワークである。

【0065】管理ネットワークに直接収容されている計算機とは、次のことを指す。ある計算機から見て外部ネットワークへの送信時に最初におよび外部からの受信時に最後に通過しなければならないセキュリティゲートウェイが存在するが、その計算機はそのセキュリティゲートウェイの管理ネットワークに直接収容されている(そのセキュリティゲートウェイが直接管理している)ものとする。例えば図1の計算機ネットワークでは、計算機H3は管理ネットワークA1に直接収容されており、計算機H4は管理ネットワークAに直接収容されている。

【0066】本発明を適用する計算機ネットワークでは、パケットが送信元のホストから最終的な宛先ホストに到達するまでに幾つかのセキュリティゲートウェイを通過する。各セキュリティゲートウェイには、そこから外部へのパケット送出あるいは外部からのパケット流入にあたり、必要に応じてパケットの認証処理(認証情報の付与や検査)を実行する。

【0067】本発明1は、パケットの認証機能に関するものであり、パケットの通過パスに存在するセキュリティゲートウェイの間で通過パスに沿った形式でリンク・バイ・リンクに認証鍵を共有する。さらに、送信ホストを直接収容するネットワークのセキュリティゲートウェイ(これを発信側ゲートウェイと呼ぶことにする)は最終宛先ホストを直接収容するネットワークのセキュリティゲートウェイ(これを宛先側ゲートウェイと呼ぶことにする)との間でエンド・ツー・エンドで認証鍵を共有する。

【0068】発信側ゲートウェイは、パケット・データに対して、エンド・ツー・エンドで共有した認証鍵1による認証コード1と、次のセキュリティゲートウェイとの間で共有している認証鍵2による認証コード2の2つを計算し、パケットに添付して転送する。

【0069】次のセキュリティゲートウェイは共有している認証鍵2によりパケットに添付された認証コード2を検査し、検査に通ればさらに次のセキュリティゲートウェイとの間で共有している認証鍵3によりパケットデータに対する認証コード3を生成し、パケットから認証コード2を除去し、代わりに認証コード3を添付して転送する。このようにパケット経路の間に存在するセキュリティゲートウェイでは、隣のセキュリティゲートウェイとの間でパケット認証コードの検査・生成による付け替えを繰り返しながら、パケットの転送が行われる。このことにより各セキュリティゲートウェイは、パケット

が経路に沿って隣のセキュリティゲートウェイから転送されていること、内容に改ざんがないことを確認できる。

【0070】また、宛先側ゲートウェイは、前段のセキュリティゲートウェイにより添付された認証コードの他に、発信側ゲートウェイにより添付された認証コード1を検査する。特に、認証コード1の検査によりパケットが発信側ゲートウェイにより発信されたものであること、内容に改ざんがないことを確認できる。

【0071】本発明2は、パケットの認証機能に関するものであり、パケットの通過パスに存在する個々のセキュリティゲートウェイと発信側ゲートウェイとの間でペア単位に別々の認証鍵を共有している。発信側ゲートウェイは、それぞれの認証鍵を用いて複数の認証コードを生成し、全てをパケットに添付して転送する。

【0072】パケットの経路に存在するセキュリティゲートウェイは、自らの装置に対応する認証コードの検査を行い、検査に通ればパケットを転送する。このことにより、パケットが発信側ゲートウェイにより発信されたものであること、内容に改ざんがないことを各経路上のセキュリティゲートウェイが確認できる。

【0073】本発明3は、パケットの暗号化機能に関するものであり、複数の計算機ネットワーク間で、データを通信する際に、通信データパケットを暗号化するセキュリティゲートウェイであって、各セキュリティゲートウェイは、自装置に直接接続されている計算機群のアドレス情報を管理する手段と、通過するデータパケットの送信元が自装置に直接接続されている計算機であるかどうかを判断する手段と、通過するデータパケットの受信先が自装置に直接接続されている計算機であるかどうかを判断する手段とを備え、通過するデータパケットの送信元が自装置に直接接続されている計算機であると判断された場合にのみデータを暗号化し、通過するデータパケットの受信先が、自装置に直接接続されている計算機であると判断された場合にのみデータを復号化するようにしたものである。

【0074】本発明4は、パケットの暗号化機能に関するものであり、複数の計算機ネットワーク間で、データを通信する際に、通信データパケットを暗号化するセキュリティゲートウェイであって、各セキュリティゲートウェイは、自装置が暗号化を行った際にデータパケットに暗号化完了を示す情報と自装置による署名情報とを付加する手段と、通過するデータパケットの暗号化完了を示す情報を検査し、もし暗号化完了でありデータに署名情報が付加されている場合には自装置では暗号化を行わないように制御し、もし暗号化完了でありデータに署名情報が付加されていない場合にはエラーを通知し、もし暗号化未完了であり、データに署名情報が付加されていない場合には、データを暗号化し、データ内に暗号化完了情報と自装置による署名情報を付加するように制御

し、もし暗号化未完了であり、かつデータに署名情報が付加されている場合にはエラーを通知するように制御する手段と、自装置に直接接続されている計算機群のアドレス情報を管理する手段とを備え、データ到達先では、発明3のように、受信先計算機が、自装置に直接接続されている計算機であると判断された場合にのみデータを復号化するようにしたものである。

【0075】以下、本実施形態をさらに詳しく説明する。

【0076】図1は、本発明の一実施形態に係るセキュリティゲートウェイが用いられる計算機ネットワークの一構成例を示す。この計算機ネットワークは、複数の組織ネットワークを相互接続するインターネットなどの外部ネットワーク101、組織Aネットワーク102、組織Bネットワーク103、組織Cネットワーク104、組織Dネットワーク105、組織Aネットワーク内の部所ネットワークA1、A2、A3、部所ネットワークA1内の部所ネットワークA11、組織Bネットワーク内の部所ネットワークB1、B2からなる。

【0077】また、本発明の一実施形態に係るセキュリティゲートウェイとして、組織A用(GA)、部所A1用(GA1)、部所A11用(GA11)、組織B用(GB)、部所B1用(GB1)、組織C用(GC)、組織D用(GD)が、それぞれ図1の位置に配置される。

【0078】このようにセキュリティゲートウェイは、保護すべきネットワークとその外部のネットワークとの接続点に設置され、その保護ネットワーク内からの送信パケットおよび保護ネットワーク内への受信パケットは共にセキュリティゲートウェイを通過しなければならないように配置され、ファイアウォールと同様の機能を果たす。ファイアウォールとは、内部ホストから外部へのサービス要求と外部から内部ネットワークへのサービス要求を共に許可されたもの以外制限するものである。

【0079】なお、本実施例では、図1における「部所ネットワーク」を、本セキュリティゲートウェイで保護されたネットワークを単位に定義している。

【0080】まず最初に本発明のセキュリティゲートウェイの認証機能について説明する。

【0081】セキュリティゲートウェイの管理する対象である管理ネットワークとは、セキュリティゲートウェイの保護対象となるネットワークをいう。例えば図1の計算機ネットワークでは、セキュリティゲートウェイGA1の管理ネットワークは部所A1ネットワークであり、セキュリティゲートウェイGA11の管理ネットワークは部所A11ネットワークである。

【0082】さらに、管理ネットワークに直接収容されている計算機とは、次のことを指す。計算機から見て外部への送信時に最初におよび外部からの受信時に最後に通過しなければならないセキュリティゲートウェイが存

在するが、そのセキュリティゲートウェイの管理ネットワークに直接収容されていると定義する。例えば図1の計算機ネットワークでは、管理ネットワークA1に直接収容されている計算機は例えばH3であり、計算機H4は管理ネットワークAに直接収容されている。

【0083】なお、図1におけるホストH5はセキュリティゲートウェイの存在しないネットワークに接続されている。このようなホストH5と安全に通信を行う場合には、ホストH5自体がセキュリティゲートウェイの機能を備えている必要がある。

【0084】図2は、図1のネットワークにおけるパケットの流れの一例を説明するための図である。図1における部所ネットワークA11内の計算機（ホストとも呼ぶ）H1から部所ネットワークB1内のホストH2宛てに送出されるパケットは、送信ホストH1→セキュリティゲートウェイGA11→GA1→GA→GB→GB1→受信ホストH2の経路を通る。

【0085】本実施形態では、ホストH2からホストH1宛てのパケットは、先の経路の逆順に流れる。ただし、場合によってはセキュリティゲートウェイを保護ネットワークに複数設置することも可能であり、その場合にはパケットの送信方向や通信相手により経由するセキュリティゲートウェイが異なることもある。

【0086】このようにパケット転送経路上に送信側と受信側で対のセキュリティゲートウェイに限定されず、複数のセキュリティゲートウェイが存在する場合、従来では、個々のセキュリティゲートウェイがどのように連携してパケットを認証すれば良いかといった問題が発生する。本セキュリティゲートウェイでは、このような状況に対処し、各々のセキュリティゲートウェイがパケットの正当性を確認しながら自らの管理するネットワークを保護可能とするものである。

【0087】まず、第1の実施形態を説明する。

【0088】図3に、本実施形態に係るセキュリティゲートウェイの構成例を示す。図3のように、セキュリティゲートウェイ310は、パケット受信部301、認証コード検査部302、認証鍵管理部303、パケットフィルタリング部304、認証コード生成部305、パケット整形部306、パケット転送部307を備えている。

【0089】パケット受信部301は、セキュリティゲートウェイ310の保護するネットワークを経由するパケットを受信する。

【0090】認証鍵管理部303は、認証鍵テーブルを管理し、認証コードの生成に用いられる証明用認証鍵、認証コードの検査に用いられる検査用認証鍵を記憶している。

【0091】認証コード検査部302は、認証鍵管理部303から得た検査用認証鍵を用いて、受信パケットの認証コードの正当性を検査する。

【0092】パケットフィルタリング部304は、受信されたパケットに含まれる送信元ホスト識別情報、受信先ホスト識別情報、コネクション識別情報を元にパケットの転送を認めるかどうかの判定を行う。

【0093】認証コード生成部305は、認証鍵管理部303から得た証明用認証鍵を用いて、次の転送先での検査に用いられる認証コードを生成する。

【0094】パケット整形部306は、パケットに添付され既に検査された認証コードの除去と新たに生成された認証コードの添付を行う。

【0095】パケット転送部307は経路情報に基づいてパケットの転送を行う。

【0096】なお、以上の構成部分のうち、パケットフィルタリング部304については、本セキュリティゲートウェイとは別にパケットフィルタリング装置として用意し、（パケットフィルタリング部304を除いた）セキュリティゲートウェイとパケットフィルタリング装置とが連係をとる形態にしても良い。この場合、セキュリティゲートウェイでは、認証コード検査部302の出力が認証コード生成部305の入力に結線された構造となる。

【0097】認証コード（MESSAGE AUTHENTICATION CODE：略してMACと呼ばれる）の計算は、例えば次のような方法を用いる。第1の方法は、秘密鍵暗号であるDES（DATA ENCRYPTION STANDARD）のCBC（CIPHER-BLOCK-CHAINING）モードでパケットデータを暗号化し、その暗号文の最終ブロックである64ビットデータを用いる方法（ISO/IEC JTC1/IS 9797に詳細な説明がある）である。第2の方法は、ハッシュ関数であるMD5（MESSAGE DIGEST ALGORITHM 5）を用いて、パケットデータの前後に認証鍵を連結したデータを、圧縮した結果である、128ビットデータを用いる方法（IETF RFC1828に詳細な説明がある）などによる。

【0098】認証コードは、パケット内のフィールドにおいて転送途中で変化するもの（例えば、ルータに到着するごとにデクリメントされるTTL（TIME-TO-LIVE）フィールドなど）を除いた全てのデータを反映したものとする。

【0099】ここで、認証コードの生成・検査に用いられる認証鍵の設定単位について説明する。第1の方法は、送信元ホストアドレス、受信先ホストアドレスの組に対して1つの認証鍵を設定することである。この場合には、同一ホスト間のパケットはどんなサービスでも同じ認証鍵によって認証コードが生成されることになる。

【0100】第2の方法は、送信元ホストアドレス、受信先ホストアドレス、送信元のポート番号、受信先のポート番号の組に対して設定することである。この場合、ポート番号の組はコネクションに対応するので、通信セッション単位に認証鍵を定義したことになる。

【0101】以下の説明では、送信ポート番号と受信先

ポート番号といった情報をコネクションIDと定義して説明を行ない、認証鍵はコネクション単位に設定されるものと仮定する。ただし、他の設定単位でも同様な適用が可能である。

【0102】図4に、転送されるパケット・フォーマットの一例を示す。パケットは、送信元ホストアドレス（図中1501）、受信先ホストアドレス（1502）、コネクションID（1503）、認証コード（1504）、データ部（1505）の各領域を備える。認証コード（1504）は複数を添付することも可能であり、その場合には個々の認証コードを識別するための通し番号や認証コードIDがさらに付けられても良い。

【0103】図5に転送されるパケットフォーマットのより詳細な一例を示す。パケットのうち、データ部（図中のData）とIPヘッダ1（図中のIP1）が送信元ホストから送出されるIPパケットである。このIPヘッダ1に送信元ホストアドレス、受信先ホストアドレスが含まれている。また認証コードは認証ヘッダ（AH）に含まれる。パケットに複数の認証コードを添付する場合には複数の認証ヘッダを用いる。認証ヘッダ（Authentication Header）はIETF RFC1826に詳しい。図5には認証ヘッダ1（図中のAH1）の外側にIPヘッダ2（図中のIP2）が、また認証ヘッダ2（図中のAH2）の外側にIPヘッダ3（図中のIP3）が挿入されている。これはIPヘッダ3により指定された宛先のノードで認証ヘッダ2内の認証コードが検査され、IPヘッダ2により指定された宛先のノードで認証ヘッダ1内の認証コードが検査されることを意味する。

【0104】例えば、図2に示した各ノードを介して送信元ホストH1がパケットを受信先ホストH2に送信する場合、ホストH1では、IPヘッダ1はソースアドレス＝ホストH1、宛先アドレス＝ホストH2と設定したパケット（IPヘッダ1とData部）を送る。セキュリティゲートウェイGA11ではこのパケットを受信し、認証ヘッダ1とIPヘッダ2を追加する。ここでIPヘッダ2のソースアドレス＝ゲートウェイGA11、宛先アドレス＝ゲートウェイGB1とする。さらに、このパケットに認証ヘッダ2とIPヘッダ3を追加する。IPヘッダ3のソースアドレス＝GA11、宛先アドレス＝GA1とする。以下、パケットの中継を行うセキュリティゲートウェイではIPヘッダ3の内容を変更しながら、パケットを転送する。このとき各中継ゲートウェイでは認証ヘッダ2の検査・除去と新たな認証ヘッダ2の作成・添付が行われる。

【0105】図6に、認証鍵管理部303に記憶される認証鍵テーブルの一例を示す。認証鍵テーブルには、送信元ホストアドレス、受信先ホストアドレス、コネクションIDの組に対して検査用認証鍵と証明用認証鍵が登録される。検査用認証鍵と証明用認証鍵のどちらか一方

は空欄の場合がある。すなわち、送信ホストが管理ネットワーク内にあれば検査用認証鍵は空欄となる。このとき、証明用認証鍵は最大2つが登録されることになる。一方、受信ホストが管理ネットワーク内であれば生成用認証鍵が空欄で、検査用認証鍵は最大2つが登録される。なお、検査用認証鍵と証明用認証鍵の両方が空欄となることはない。複数のセキュリティゲートウェイでの認証鍵の配送・共有方法については後で例を説明する。

【0106】以上のような装置がどのように連係してパケット転送を行うかを図7の例を基に説明する。前提として、パケット転送経路上のセキュリティゲートウェイであるGA11、GA1、GA、GB、GB1の間では次のように認証鍵を共有しているものとする。すなわち、GA11とGA1の間で認証鍵K1、GA1とGAの間で認証鍵K2、GAとGBの間で認証鍵K3、GBとGB1の間で認証鍵K4、さらにはGA11とGB1の間で認証鍵K0がそれぞれ共有されている。

【0107】セキュリティゲートウェイGA11は、ホストH1から受信したパケットに指定されている送信ホスト、受信ホスト、コネクションIDを調べ、対応する認証鍵K0でパケットの内容に相当するデータに対する認証コードMAC0を計算する。同様に、認証鍵K1を用いて認証コードMAC1を計算する。この2つの認証コードをパケットに添付して転送する。このパケットはルーティング処理に従って次のセキュリティゲートウェイGA1に到着する。

【0108】セキュリティゲートウェイGA1では、受信したパケットに添付されている送信ホスト、受信ホスト、コネクションIDを調べ、対応する認証鍵K1により認証コードMAC1を検査する。MAC1の正当性が確認された場合には、認証鍵K2によりパケットデータに対する認証コードMAC2を計算し、パケットに添付されたMAC1を除去し、MAC2を添付したパケットを転送する。

【0109】以下、セキュリティゲートウェイGA、GBでは、セキュリティゲートウェイGA1と同様に認証コードの検査、認証コードの生成と置き換えを行いながらパケットを転送する。異常がなければパケットはセキュリティゲートウェイGB1に到達する。

【0110】セキュリティゲートウェイGB1では、まず、MAC4を認証鍵K4で検査し、これに以上がなければMAC0を認証鍵K0で検査する。この検査に以上がなければ、受信したパケットはホストH1を収容するネットワークから発信され、途中で改ざんされることなく上位のセキュリティゲートウェイGBを経由して受信されたことが確認される。最後に、MAC4とMAC0を除去したパケットをホストH2に転送することでパケットの転送は完了する。

【0111】なお、本実施形態の変形例として、セキュリティゲートウェイGBとGB1の間では認証鍵K4を

共有せずに、GBではGAから転送されたパケットのMAC3を検査し、検査結果が異常でないときにはMAC3を取り除いたパケット(MAC0が付加されているだけのパケット)をGB1に転送するようにしても良い。この場合、GB1では認証鍵K0を用いてMAC0を検査するのみとなる。上述のセキュリティゲートウェイGBがMAC4を付ける実施形態は、受信パケットがセキュリティゲートウェイGBを経たものであることを最初に確認した上で、ホストH1を収容するネットワークのセキュリティゲートウェイGA11から発信されたものであることを確認する方式となるが、セキュリティゲートウェイGB1にとって特に重要なのはGA11からの発信パケットであることの確認であるから、余分なMAC4の検査を省略しても良い。

【0112】さらに、外部からの管理ネットワークへの不正な侵入の防止だけを目的とする場合には、パケットの発信側のネットワークにおいて、セキュリティゲートウェイGA11とGA1の間でのMAC1の生成・検査、およびセキュリティゲートウェイGA1とGAの間でのMAC2の生成・検査は不要である。具体例としては、セキュリティゲートウェイGA11が鍵K0を用いてパケットにMAC0を添付し、セキュリティゲートウェイGA1はパケットが外向き(すなわち内部ネットワークから外部ネットワーク向き)か内向き(すなわち外部ネットワークから内部ネットワーク向き)かだけを検査し、外向きの場合にはそのまま転送する。セキュリティゲートウェイGA1はパケットが外向きか内向きかを検査し、外向きであれば鍵K3でMAC3を生成し、パケットに添付する。この場合には鍵K1とK2の共有が不要となる。

【0113】以上に説明した第1の実施形態におけるセキュリティゲートウェイの処理手順を図8に示した。

【0114】本実施例のセキュリティゲートウェイは、パケットを受信すると(ステップS801)、まず、パケットの送信元ホストアドレスを調べ、直接収容する管理ネットワーク内ホストからの送信かどうかを検査する(ステップS802)。これは原理的には、セキュリティゲートウェイが管理ネットワークに直接収容されている全てのホストのアドレスの一覧表を保持しており、それと比較することで行う。ホストのアドレスが統一的に付けられていれば、アドレスの一部を検査すればよい。例えば、直接収容しているホストのアドレスがある範囲内にあるように設定されていれば、送信元アドレスがその範囲かどうかを調べれば良い。

【0115】ステップS802の検査の結果、直接収容する管理ネットワーク外のホストからの送信であれば、受信パケットには認証コードが添付されているはずであるから、認証コードの検査処理であるステップS803からS806の処理を行う。一方、そうでない場合、認証コードは添付されていないので、ステップS80

7以降の処理に移る。

【0116】認証コードの検査処理においては、まず、認証コードがパケットに添付されているかどうかを調べる(ステップS803)。

【0117】認証コードが添付されていない場合には、不正な通信パケットと判断してエラー処理に移る(ステップS812)。エラー処理の一例は、受信パケットの転送を行わず、ログに記録を残すことである。

【0118】認証コードが添付されている場合には、認証コードの検査を行う(ステップS804)。このとき図6に示した認証鍵テーブルの送信元ホスト、受信先ホスト、コネクションIDのエントリを調べ、検査用の認証鍵を用いる。認証コードの検査の結果、異常があればエラー処理に移る(ステップS812)。異常がなければ、受信パケットは正常とみなす。なお、ステップS803からS805までの認証コードの検査は、認証鍵テーブルの該当エントリに登録されている検査用認証鍵の個数だけ行う。

【0119】そして、全ての認証コードが正当な場合のみステップS806に移り、ここで検査した全ての認証コードを除去する。

【0120】ここまででパケットの完全性(ホストアドレスやポート番号などが改ざんされておらず、正規の送信ホストからのものであること)が確認されたので、ステップS807のパケットフィルタリング処理を行う。

【0121】ステップS807のパケットフィルタリング処理では、送信側と受信側双方のホストアドレス、ポート番号などを基にパケットの通過を認めてよいかどうかを判定する。この判定は、例えば、フィルタリングのルールを記述したテーブルを用意し、そのルール群と逐一照合することで行う。フィルタリング処理で通過を許可されないパケットに対しては転送を行わず、その行為をログに残すなどの処理を行う。なお、前述したようにパケットフィルタリング部304は別装置の機能に委ねることも可能であり、この場合にはこの処理は省略される。

【0122】次に、受信先ホストのアドレスから、直接収容する管理ネットワーク内ホストへの受信パケットかどうかを判断する(ステップS808)。そうであれば、そのままパケットの転送処理を行う(ステップS811)。

【0123】一方、直接収容する管理ネットワーク外のホストへの受信パケットの場合には、以下の認証コードの生成処理に移る。認証コードの生成では、認証鍵テーブルから証明用の認証鍵を求め、該当エントリに登録されている全ての認証鍵を用いた認証コードを生成し(ステップS809)、それらをパケットに添付する(ステップS810)。その後、パケット転送を行う(ステップS811)。

【0124】以上の説明では、認証コードの生成・検査

において転送途中で変化する特定のエリア以外の全てのビットを対象に認証コードを計算することを想定した。これは必ずしも必要ではない。この実施形態では、エンド・ツー・エンドの認証コードとリンク・バイ・リンクの認証コードが併用されている。エンド・ツー・エンドでは送信されたパケットが1ビットも改変されることなく受信されたことを保証する必要があるが、リンク・バイ・リンクでは必ずしも全てのビットが改変なく受信されたことまで保証する必要はなく、そのパケットの転送に隣のセキュリティゲートウェイが関与したことを保証すれば十分であるとも考えられるからである。

【0125】このリンク・バイ・リンクの認証子の生成対象のデータを図4のフォーマットで説明すれば、送信元ホストアドレス(1501)、受信先ホストアドレス(1502)、コネクションID(1503)、さらにエンド・ツー・エンドの認証コード(1504)までを対象にすればよい。

【0126】また、図5のフォーマットで説明すると、認証ヘッダ1(図中のAH1)がエンド・ツー・エンドの認証コードを含むため、この中の認証コードの計算はIPヘッダ2(図中のIP2)、認証ヘッダ1(ただし認証コードのエリアは“0”で置き換える)、IPヘッダ1(図中のIP1)、データ部(図中のData)を対象とする。一方、認証ヘッダ2(図中のAH2)はリンク・バイ・リンクの認証コードを含むが、この部分の認証コードの計算はIPヘッダ3(図中のIP3)、認証ヘッダ2、認証ヘッダ1を対象にすればよい。この認証コード1、2とその保護対象のデータの関係を図9に示した。

【0127】なお、このときにリンク・バイ・リンクの認証コードによる保護の対象は、図9にハッチングして示した領域の全てを含まなければならない訳ではない。少なくとも含めなければならないのは、エンド・ツー・エンドの認証コードの保護の対象外であるIPヘッダ3と認証ヘッダ2である。さらに、エンド・ツー・エンドの認証コードの保護対象のデータのうち毎回変化するデータを含めなければならない。例えば、必ずカウントアップされるシーケンス番号や、あるいは十分な長さのランダムなデータである。十分な長さとは例えば128ビットである。エンド・ツー・エンドの認証コードは、実用上128ビットのランダムデータと見なすことが可能であるため、先の説明ではこの認証コードを含む認証ヘッダ1を対象に含めている。

【0128】このようにした場合のパケット転送処理の一例を図7で説明すると、MAC1、MAC2、MAC3、MAC4の生成・検査が効率化され、パケット転送の効率化につながる効果がある。

【0129】以上に示したメッセージ認証コードの多重化は、この第1の実施形態のみならず以降で説明する第2の実施形態などにも適用可能である。

【0130】次に、第2の実施形態について説明する。

【0131】本実施形態では、セキュリティゲートウェイの構成は、送信元のネットワークに接続されたセキュリティゲートウェイ(図10)とそのパケットの転送経路上のセキュリティゲートウェイ(図11)の2種類に分けられる。ただし、図10の構成と図11の構成の必要部分を融合させて一つのセキュリティゲートウェイとした構成も考えられ、その場合には図3と同様の構成になる。

【0132】図10に示したように本実施形態に係る送信元のセキュリティゲートウェイ510は、パケット受信部501、パケット転送部502、認証鍵管理部503、認証コード生成部504、パケット整形部505、パケットフィルタリング部506を備える。

【0133】パケット受信部501は、セキュリティゲートウェイ510の保護するネットワークから発信されるパケットを受信する。

【0134】パケットフィルタリング部506は、受信されたパケットに含まれる送信元ホスト識別情報、受信先ホスト識別情報、コネクションID、および認証コードを元にパケットの転送を認めるかどうかなどの制御を行う。

【0135】認証鍵管理部503は、送信元ホスト識別情報、受信先ホスト識別情報、コネクションIDの3つ組データに対応する証明用認証鍵を登録したテーブルを管理する。このとき、同一の3つ組データに対し、生成用認証鍵が複数記憶されている点の特徴である。これらの証明用認証鍵は、パケットが通過するセキュリティゲートウェイと1つずつ共有されている。

【0136】認証コード生成部504は、認証鍵管理部503から得た複数の証明用認証鍵を用いて、パケットの転送先での検査に用いられる複数の認証コードを生成する。

【0137】パケット整形部505は、認証コード生成部504により得られる複数の認証コードを、転送経路での検査の順番に従ってパケットに添付する。

【0138】パケット転送部502は、経路情報に基づいてパケットの転送を行う。

【0139】図11に示したように本実施形態に係る転送経路上のセキュリティゲートウェイ(送信元以外のもの)610は、パケット受信部601、パケット転送部602、認証鍵管理部603、認証コード検査部604、パケット整形部605、パケットフィルタリング部606を備える。

【0140】パケット受信部601、パケット転送部602、パケットフィルタリング部606の構成・動作は、図6および図10と同様である。相違するのは、以下の点である。認証鍵管理部603が送信元ホストアドレス、受信先ホストアドレス、コネクションIDの3つ組データに対応する検査用認証鍵(1つ)を登録したテ

ーブルを管理しており、認証コード検査部604はこの検査用認証鍵を用いてパケットに添付されている認証コードを検査する。パケット整形部605は、このセキュリティゲートウェイで検査された認証コード1つを除去する。

【0141】なお、図10と図11の構成部分のうち、パケットフィルタリング部506や606はセキュリティゲートウェイとは別にパケットフィルタリング装置を用意し、セキュリティゲートウェイとパケットフィルタリング装置とが連係をとる形態にしても良い。この場合、パケットフィルタリング部506や606は不要となる。

【0142】次に、本セキュリティゲートウェイを用いたパケット転送の流れを図12を用いて説明する。

【0143】前提として、パケット転送経路上のセキュリティゲートウェイであるGA11、GA1、GA、GB、GB1の間では次のように認証鍵を共有しているものとする。すなわち、GA11とGA1の間で認証鍵K1、GA11とGAの間で認証鍵K2、GA11とGBの間で認証鍵K3、GA11とGB1の間で認証鍵K4がそれぞれ共有される。

【0144】セキュリティゲートウェイGA11は、受信したパケットに指定されている送信元ホストアドレス、受信先ホストアドレス、コネクションIDを調べ、対応する認証鍵K1でパケットの内容に相当するデータに対する認証コードMAC1を計算する。同様に、認証鍵K2、K3、K4を夫々用いて認証コードMAC2、MAC3、MAC4を計算する。これら4つの認証コードを全てパケットに添付して転送する。

【0145】このパケットはルーティング処理に従って次のセキュリティゲートウェイGA1に到着する。

【0146】セキュリティゲートウェイGA1では、受信したパケットに指定されている送信元ホストアドレス、受信先ホストアドレス、コネクションIDを調べ、対応する認証鍵K1により認証コードMAC1を検査する。ここで、認証コードMAC1が添付されていない場合やMAC1の正当性が確認されない場合にはエラー処理に移る。MAC1の正当性が確認された場合には、パケットに添付されたMAC1を除去してパケットを転送する。

【0147】以下、セキュリティゲートウェイGA、GBではセキュリティゲートウェイGA1と同様に認証コードの検査と除去を行いながらパケットを転送する。異常がなければパケットはセキュリティゲートウェイGB1に到達する。

【0148】セキュリティゲートウェイGB1では、MAC4を認証鍵K4で検査し、これに異常がなければ、受信したパケットはホストH1を収容するネットワークから発信され、途中で改ざんされることなく受信されたことが確認される。最後にMAC4を除去したパケット

をホストH2に転送することでパケットの転送は完了する。

【0149】なお、本実施形態の変形例として、外部からの不正な侵入の防止だけを目的とする場合には、パケットの発信側のネットワークにおいて、セキュリティゲートウェイGA11とGA1の間でのMAC1の生成・検査、およびセキュリティゲートウェイGA1とGAの間でのMAC2の生成・検査は不要である。具体例としては、セキュリティゲートウェイGA11とGBが鍵K3を共有し、GA11とGB1が鍵K4を共有しておく。セキュリティゲートウェイGA11はパケットに対し、鍵K3で認証コードMAC3を、鍵K4で認証コードMAC4をそれぞれ生成し、パケットに添付して転送する。セキュリティゲートウェイGA1とGAではパケットの方向だけを監視し、方向が外向きならばそのまま転送する。以下、セキュリティゲートウェイGBとGB1の処理は元の実施形態と同じである。この場合には鍵K1とK2の共有が不要となる。

【0150】さらに、元の実施形態や上記の変形例において、転送経路上のセキュリティゲートウェイにおいて、検査された認証コードの除去を行わない構成があげられる。この場合、検査された認証コードの除去は行わないため、パケットの長さは送信元のセキュリティゲートウェイ（図12の例ではGA11）から受信先のセキュリティゲートウェイ（図12の例ではGB1）まで不変である。

【0151】図13にセキュリティゲートウェイ内の認証鍵管理部503、603に登録されている認証鍵テーブルの一例を示す。認証鍵テーブルには送信元ホストアドレス、受信元ホストアドレス、コネクションIDの組に対して検査用認証鍵と証明用認証鍵が登録される。検査用認証鍵と証明用認証鍵のどちらか一方は常に空欄であるが、両方が空欄となることはない。すなわち、送信ホストが管理ネットワーク内にあれば検査用認証鍵は空欄となり、証明用認証鍵は一般に複数登録されるが、最大でも経路に存在する他のセキュリティゲートウェイの個数だけとなる。それ以外の場合で、自らのセキュリティゲートウェイが経路上にある場合には、検査用認証鍵が1つ登録される。

【0152】以上に説明した第2の実施形態におけるセキュリティゲートウェイの処理手順を図14に示した。

【0153】本実施形態のセキュリティゲートウェイは、パケットを受信すると（ステップS901）、まず、パケットの送信元ホストアドレスを調べ、直接収容する管理ネットワーク内ホストからの送信かどうかを判断する（ステップS902）。

【0154】直接収容する管理ネットワーク外のホストからの送信であれば、ステップS903からS906の認証コードの検査を行う。

【0155】まず、受信パケットに認証コードが添付さ

れているかどうかを調べる（ステップS903）。認証コードが添付されていない場合には、不正な通信パケットと判断してエラー処理に移る（ステップS909）。認証コードが添付されている場合には、認証コードの検査を行う（ステップS904）。このとき認証鍵テーブルの送信ホスト、受信ホスト、コネクションIDのエントリを調べ、検査用の認証鍵を用いる。認証コードの検査の結果異常があればエラー処理に移る（ステップS909）。異常がなければ受信パケットは正常とみなし、検査した認証コードを除去し（ステップS906）、パケットのフィルタリング処理を行なう（ステップS907）。フィルタを通過したパケットのみを転送する（ステップS908）。

【0156】一方、ステップS902において直接収容する管理ネットワーク内ホストからの送信の場合には、さらに受信ホストも直接収容する管理ネットワーク内かどうかを判断する（ステップS907）。もしそうであれば管理ネットワーク内の通信パケットなのでセキュリティゲートウェイは何も処理を行わずに終了する。

【0157】受信ホストが直接収容する管理ネットワークの外の場合には、まずパケットのフィルタリング処理を行なう（ステップS911）。フィルタを通過したパケットに対してステップS912からS913の認証コード生成処理を行う。このとき、図13に示した認証鍵テーブルに記録された全ての認証鍵を用いて複数の認証コードを生成し（ステップS912）、生成した全ての認証コードをパケットに添付して（ステップS913）、パケットを転送する（ステップS914）。なお、先に説明したようにパケットフィルタリング部506、606は別装置の機能に委ねることも可能であり、この場合にはフィルタリング処理（ステップS907、S911）は省略される。

【0158】次に、経路上のセキュリティゲートウェイの処理量を削減する実施形態を幾つか説明する。

【0159】図15に、第3の実施形態におけるパケット転送の流れを示す。

【0160】第3の実施形態は、第1の実施形態を変形したものに相当し、例えば図7の例において転送経路上のセキュリティゲートウェイ（GA1、GA、GB）で検査するための認証コード（これを通過用認証コードと呼ぶことにする）は全て同一とし、一方エンドのセキュリティゲートウェイでは別途エンド・ツー・エンドの認証コード（これを受信用認証コードと呼ぶことにする）を検査することにする。従って、例えば図15のように、送信側ゲートウェイであるGA11は証明用認証鍵K0とK1を所持し、宛先側ゲートウェイであるGB1は検査用認証鍵K0（さらには検査用認証鍵K1）を所持し、経路上のセキュリティゲートウェイであるGA1、GA、GBは検査用認証鍵K1を共有する。

【0161】送信側ゲートウェイは、パケットに対し、

受信用認証コードMAC0と通過用認証コードMAC1を生成し、パケットに添付して送信する。経路上のセキュリティゲートウェイは通過用認証コードMAC1のみを検査し、検査に通ればそのままパケットを転送する。最後に受信側ゲートウェイは、受信用認証コードMAC0（さらには通過用認証コードMAC1）を検査し、検査に通れば認証コードを除去して受信ホスト宛に転送する。

【0162】本実施形態では、送信側ゲートウェイは図10と同じ構成であり、受信側ゲートウェイは図11と同じ構成である。転送経路上のセキュリティゲートウェイは図11においてパケット整形部605のない構成となる。

【0163】図16および図17に、第3の実施形態によるセキュリティゲートウェイの処理手順を示す。

【0164】本セキュリティゲートウェイは、パケットを受信すると（ステップS1301）、最初にパケットの送信元ホストアドレスを調べ、直接収容する管理ネットワーク内ホストからの送信かどうかを判断する（ステップS1302）。

【0165】直接収容する管理ネットワーク外のホストからの送信であれば、以下の認証コードの検査処理を行う。

【0166】まず、パケットの受信先ホストアドレスを調べ、直接収容する管理ネットワーク内ホストへの受信パケットかどうかを判断する（ステップS1303）。直接収容する管理ネットワーク内ホストへの受信パケットであれば、自装置は宛先側ゲートウェイであるから、ステップS1309からS1314までの受信用認証コードの検査処理を行う。受信用認証コードの検査処理では、最初に受信用認証コードの有無を検査し（ステップS1309）、受信用認証コードの検査を行う（ステップS1310）。これに異常がなければ認証コード（通過用も受信用も全て）を除去し（ステップS1312）、フィルタリング処理（ステップS1313）を行い、フィルタを通過したパケットのみを転送する（ステップS1314）。

【0167】一方、直接収容する管理ネットワーク外ホストへのパケットであれば、自装置は経路上となるのでステップS1304からS1308までの通過用認証コードの検査処理を行う。通過用認証コードの検査処理では、最初に通過用認証コードの有無を検査し（ステップS1304）、通過用認証コードの検査（ステップS1305）を行う。これに異常がなければフィルタリング処理（ステップS1307）を行い、フィルタを通過したパケットのみを転送する（ステップS1308）。

【0168】上記の認証コードの検査過程（ステップS1304、S1306、S1309、S1311）で異常が発見された場合は、エラー処理（ステップS1320）を行い、終了する。

【0169】また、ステップS1302の判定において直接収容する管理ネットワーク内のホストからの送信であれば、受信アドレスを調べ、受信先も直接収容する管理ネットワーク内かどうかを調べる（ステップS1315）。もしそうであれば、直接収容する管理ネットワーク内での送受信であるので何もせずに終了する（ステップS1321）。

【0170】受信先が直接収容する管理ネットワーク外であれば、自装置は送信側ゲートウェイであるからステップS1316からS1319までの認証コード生成処理を行う。まず、パケットのフィルタリング処理（ステップS1316）を行い、フィルタを通過したパケットに対して認証コードの生成処理を行う（ステップS1317）。そして、生成した認証コードをパケットに添付して（ステップS1318）、転送する（ステップS1319）。このとき、経路上に宛先側ゲートウェイ以外が存在しない場合以外は、2種類の認証コード（受信用認証コードと通過用認証コード）を生成する。

【0171】なお、先に説明したようにパケットフィルタリング部は別装置の機能に委ねることも可能であり、この場合にはフィルタリング処理（ステップS1307、S1313、S1316）は省略される。

【0172】第4の実施形態は、転送経路上のセキュリティゲートウェイの認証処理をさらに簡略化するものである。図18にホストH1からホストH2へのパケット転送とそのときの認証処理を例示した。前提として、ホストH1、H2を収容する管理ネットワークのセキュリティゲートウェイGA11、GB1が認証鍵Kを共有しているものとする。また、各セキュリティゲートウェイは他のセキュリティゲートウェイのネットワーク上の位置を把握しており、受信先ホストアドレスからその管理ネットワークのセキュリティゲートウェイのアドレスの対応が分かるものとする。例えば、通信可能な全てのホストアドレスとそれに対応するセキュリティゲートウェイの一覧をテーブルに管理しているものとする。

【0173】まず、ホストH1からパケットを受信したセキュリティゲートウェイGA11は受信先ホストアドレスH2からそれに対応するセキュリティゲートウェイGB1のアドレスを求める。次に、パケット全体をデータとみなして、送信元アドレスとしてセキュリティゲートウェイGA11のアドレス、受信先アドレスとしてセキュリティゲートウェイGB1のアドレスを添付したパケットを作成する。この処理はカプセル化と呼ばれる。さらに、認証鍵Kで元の受信パケットに対する認証コードを計算し、これをカプセル化したパケットに添付して転送する。

【0174】パケットはルーティング処理によりセキュリティゲートウェイGA1に到着するが、セキュリティゲートウェイGA1では受信先のアドレスがセキュリティゲートウェイであることを認識すると、そのまま転送

する。このパケットは同様にしてセキュリティゲートウェイGA、GBに到着するが、これらも受信先がセキュリティゲートウェイであればそのまま転送する。

【0175】最後にカプセル化されたパケットの宛先であるセキュリティゲートウェイGB1ではまず送信元アドレス、受信先アドレス、認証コードなどのヘッダを除き去してデカプセル化を行い、その後のパケットに対して認証鍵Kで認証コードを検査する。認証に成功すればパケットを転送してホストH2に届ける。

【0176】これは、宛先がセキュリティゲートウェイであれば、宛先側ゲートウェイでパケットの正当性が検査されるため、途中のセキュリティゲートウェイでは正当性の検査を簡略化したものである。

【0177】ここで、複数のセキュリティゲートウェイの間で認証鍵を共有する方法の一例を示す。

【0178】以下で説明する方法は公開鍵暗号をベースにしている。前提として、各セキュリティゲートウェイには固有の秘密鍵と公開鍵が割り当てられているものとする。また、各セキュリティゲートウェイはネットワーク内での全てのセキュリティゲートウェイの位置を把握しており、パケットを転送するにあたりどのセキュリティゲートウェイを経由して受信先まで届くかが分かっているものとする。さらに、全てのセキュリティゲートウェイの公開鍵を登録したテーブルを所持しているものとする。

【0179】このような前提の下で、送信側のセキュリティゲートウェイが認証鍵をランダムに決定し、受信側のセキュリティゲートウェイの公開鍵で暗号化したデータを作成し、パケットと一緒に転送する。受信側では自らの秘密鍵でこれを復号して認証鍵を得る。

【0180】具体的には、第1の実施形態（図7）において、GA11が認証鍵K0とK1を決定し、K0をGB1の公開鍵で暗号化したデータCK0と、K1をGA1の公開鍵で暗号化したデータCK1を計算し、これらをコネクション確立時の最初のパケットに添付して送信する。このパケットを受信したGA1はCK1を自分の秘密鍵で復号して認証鍵K1を得る。さらにGA1は認証鍵K2をランダムに決定し、K2をGAの公開鍵で暗号化したデータCK2を作成し、パケットからCK1を削除しCK2を添付して送信する。以上のことをセキュリティゲートウェイGB1まで行えば図7に示したようにコネクションに対応した認証鍵が共有される。

【0181】第2の実施形態（図12）でも、GA11が認証鍵K1、K2、K3、K4をランダムに決定し、これらを配布先のセキュリティゲートウェイの公開鍵で暗号化してコネクション確立のパケットに添付して転送すれば良い。このパケットを受信した各セキュリティゲートウェイは自分宛の暗号化データを自分の秘密鍵で復号して認証鍵を得る。

【0182】第3の実施形態および第4の実施形態に関

しても同様にして認証鍵を共有できる。

【0183】なお、鍵共有の前提条件を緩和するためには、例えば経路上のゲートウェイ間い合わせプロトコルを用意すればよい。すなわち、送信パケットを受信したセキュリティゲートウェイGA11が、最初に経路上のゲートウェイ間い合わせ要求を受信先に向かって発信し、この間い合わせ要求を受信した経路上のセキュリティゲートウェイが自らの公開鍵とアドレスを間い合わせパケットに添付しながら転送し、最終的に間い合わせパケットを受け取ったセキュリティゲートウェイGB1が、このパケット自体を応答として送信元のセキュリティゲートウェイGA11に向かって返すことにする。間い合わせ要求パケットを受信したセキュリティゲートウェイは、経路上の1つ手前のセキュリティゲートウェイのアドレスと公開鍵を認識できる。さらに、応答パケットをも受信することで、経路上の1つ先のセキュリティゲートウェイのアドレスと公開鍵も認識できる。

【0184】以上の説明では、セキュリティゲートウェイと送受信ホストを区別してきたが、これを同一とする構成も可能である。すなわち、送受信パケットの認証機構を一般のホストに搭載することもできる。この場合には、パケット認証機構の保護対象はそれを搭載したホストとなる。例えば、これまでに説明した第1～第4の実施形態の場合、いずれにおいても送信側ゲートウェイ（図2におけるGA11）の機能をホストH1に、宛先側ゲートウェイ（図2におけるGB1）の機能をホストH2に持たせれば良い。

【0185】次に、図19に送信側および受信側のパケット認証機構を搭載したホストの一構成を示す。

【0186】本ホストは、アプリケーション処理部1601、トランスポート処理部1602、インターネットプロトコル（IP）処理部1603、パケット認証処理部1604、ネットワークインタフェース1605から構成される。このうち、1601～1603および1605はTCP/IPによるプロトコルモジュールそのものである。

【0187】パケット認証処理部1604は、認証コード検査部1611、受信パケット整形部1612、認証鍵管理部1613、認証コード生成部1614、送信パケット整形部1615から構成される。

【0188】パケット認証処理部の動作は、送信時の処理と受信時の処理の2つに分けられる。

【0189】まず、上位層から要求のあったパケットに認証子を生成し、送信する処理においては、上位層からのパケットに添付されている送信先アドレスとコネクションIDにより認証鍵管理部1613のテーブルを検索し、そのエントリに登録されている全ての証明用認証鍵を用いてパケットに対する認証コードを生成し、それをパケットに添付する。

【0190】一方、受信したパケットの認証を行ない、

上位層に渡す処理においては、受信パケットに添付されている送信元アドレスとコネクションIDにより認証鍵管理部1613のテーブルを検索し、そのエントリに登録されている検査用認証鍵を用いて認証コードを検査する。認証に成功したパケットのみを上位層に渡す。認証に失敗したパケットに対してはエラー処理を行なう。

【0191】このようにセキュリティゲートウェイ機能を送受信ホストにて動作させる構成は移動計算機を用いるモバイル・コンピューティングにおいて必須となる。このような状況での本実施形態のセキュリティゲートウェイの動作を以下で説明する。

【0192】図1におけるホストH4が外部ネットに移動し、ホストH5の位置に移動したものとす。ホストH5の位置から元の組織Aネットのあるホストと通信するためにはセキュリティゲートウェイGAを通過するためのパケット認証子を添付したパケットを生成しなければならない。外部ネットはセキュリティゲートウェイで保護されていないため、認証子の生成・検査は移動ホスト自身が行う必要がある。

【0193】図20におけるホストH4が組織BネットのホストH2の位置に移動し、組織AネットのホストH3へパケットを送信する場合のセキュリティゲートウェイの動作例を示した。図20の例は、ホストH4からセキュリティゲートウェイGA1へのエンド・ツー・エンドの認証子MAC0とリンク・バイ・リンクの認証子MAC1をパケットに添付して送信する第1の実施例（図7）に相当するものである。図7との違いは送信ホストであるH4自身がパケット認証子を生成して送信する点にある。セキュリティゲートウェイGB1にとっては、受信したパケットの送信ホストを認証する必要がある、このために移動ホストH4が認証子MAC1を生成することを要求することになる。

【0194】セキュリティゲートウェイが移動ホストをも収容する場合、その移動ホストの正当性が確認されることは、モバイル環境でのホストのなりすましを防ぐ上で極めて重要な意味を持つ。従って、本発明の骨子である、多数のセキュリティノードを介して安全にデータを転送する方法は、移動ホストの混在するイントラネット構築において効果的である。

【0195】次に、本発明の他の実施形態に係るセキュリティゲートウェイの暗号処理機能について説明する。

【0196】以下では、このセキュリティゲートウェイ（ファイアウォール）をデータ暗号化、復号化の制御方式とそれに伴うデータパケットの形式の相違をもとに4タイプに分け、各々の実現方法を説明する。

【0197】（タイプ1）まず、図21と図22を参照しながら、本実施形態に係るセキュリティゲートウェイの構成および動作について説明する。

【0198】図21に、本実施形態のセキュリティゲートウェイ（タイプ1）の基本構成を示す。図21に示す

ように、タイプ1のセキュリティゲートウェイ2は、暗号化部11、復号化部12、暗号鍵記憶部13、ホストアドレス管理部14、ホストアドレス比較部15を備える。

【0199】図22は、本セキュリティゲートウェイを通過するデータパケットの形式の一例を示す。データパケットは、送信元ホストアドレス（図中21）、受信先ホストアドレス（22）、データ属性（23）、データ本体（24）から構成される。送信元ホストアドレス（21）は送信元ホスト計算機を、受信先ホストアドレス（22）は受信先ホスト計算機を、それぞれ一意に示す識別子で、例えばネットワークアドレスを使用する。データ属性（23）は、例えば複数のビットで構成されるフラグ情報である。なお、データ属性（23）は、タイプ1のセキュリティゲートウェイでは使用しないので、ネットワーク内にタイプ1のセキュリティゲートウェイ2のみを設ける場合には、データ属性（23）のフィールドは、他の用途で使用しない限り、不要である。

【0200】図21のセキュリティゲートウェイにおいて、暗号化部11は、データ本体（24）を暗号化する。復号化部12は、データ本体（24）を復号化する。暗号鍵記憶部13は、データの暗号化、復号化に使用される暗号鍵の管理、記憶を行う。暗号鍵記憶部13には、例えばシステム管理者によって必要な暗号鍵情報が格納される。ホストアドレス管理部14は、自セキュリティゲートウェイに直接接続されているホスト計算機のホストアドレスを格納している。ホストアドレス比較部15は、ホストアドレス管理部14内に格納されているホスト計算機のホストアドレスと、データパケット内の送信元ホストアドレス（21）および受信先ホストアドレス（22）とを比較する。

【0201】図23に、本セキュリティゲートウェイがデータパケットを受けとった際の動作を示す。もしホストアドレス比較部15にて送信元ホストアドレス21の示すホスト計算機がホストアドレス管理部14に登録されていると判断したなら（ステップS11、S12）、本セキュリティゲートウェイ2は暗号化部11でデータ本体（24）を暗号化する（ステップS13）。そして、データパケットを次段に転送する（ステップS17）。

【0202】また、ホストアドレス比較部15が、受信先ホストアドレス22の示すホスト計算機がホストアドレス管理部14に登録されていると判断したなら（ステップS14、S14）、復号化部12でデータ本体（24）を復号化する（ステップS16）。そして、データパケットを次段に転送する（ステップS17）。

【0203】また、上記以外の条件の場合には、セキュリティゲートウェイ2はデータパケットに何も処理を行わず通過させる（ステップS17）。

【0204】なお、ホストアドレス管理部14およびホ

ストアドレス比較部15でのアドレスの比較は、前述の方法の他に、このセキュリティゲートウェイの下位に構築されているサブネットワークアドレスをホストアドレス管理部14に登録しておき、これとデータパケット内の送信元ホストアドレス21および受信先ホストアドレス22とを比較するといったように、他の構成を取ることも可能である。

【0205】以上のような動作の結果、データパケットは、図24に示すように、送信元ホスト3sを出て最初のセキュリティゲートウェイ2bで暗号化され、受信先ホストの直前のセキュリティゲートウェイ2cで復号化されることになる。すなわち、データは1回のみ暗号化、復号化され、一度セキュリティゲートウェイを通過した後は暗号化されていることになる。

【0206】（タイプ2）図25に、本実施形態のセキュリティゲートウェイ（タイプ2）の基本構成を示す。タイプ2のセキュリティゲートウェイ2は、図21の構成に暗号化判定部16を付加したものである。

【0207】本セキュリティゲートウェイを通過するデータパケットの形式の一例は、先に説明した図22のものと同様である。

【0208】本セキュリティゲートウェイは、上述したタイプ1のセキュリティゲートウェイと同様の機能を、図22のデータ属性（23）に基づく処理で実現したものである。すなわち、本実施形態では、データパケット内のデータ属性（23）として1ビットの暗号化ビットをビット0（最下位ビット）に設け、その値が1の場合データは暗号化されており、0の場合は暗号化されていないこと（非暗号化）を示すものとする。暗号化判定部16にて暗号化ビットが1か0かを調べることで、容易に暗号化されているか否かを判定することができる。

【0209】ここでは、各セキュリティゲートウェイは、暗号化されていないデータパケットが来た場合、ホストアドレス管理部14を参照することなく、暗号化するようにしており、送信元を出て最初のセキュリティゲートウェイに到達した時点でデータは暗号化される。そして受信先ホストの1つ前のセキュリティゲートウェイではタイプ1と同様に、受信先ホストアドレス22の示すホスト計算機がホストアドレス管理部14に登録されているなら、復号化部12でデータ本体24を復号化する。本セキュリティゲートウェイは、先のタイプ1のものに比較し、ホストアドレス管理部14の検索、データ内のホストアドレスとの比較処理が1回で済むので、より効率の良いデータ転送が期待できる。

【0210】ただし、ここでは、データ転送の安全性を保持するために、データ暗号化ビットの転送途中での改ざんに対応することを考慮する。すなわち、転送経路でのデータ改ざんに対処するため、データを暗号化したセキュリティゲートウェイは、暗号化ビットを1にすると

同時に、データパケット内の署名フィールドを自身の署名情報（例えば、デジタル署名）で置き換える。これは、例えばデータ属性（23）の一部のフィールドを使用してもよいし、個別に設けてもよい。

【0211】もし経路途中で、何者かによって本来0（未暗号化）のデータが1（暗号化）に改ざんされた場合、署名情報は元データのままであるので、次の段階のセキュリティゲートウェイはデータの矛盾を指摘でき、エラーとして転送を中止できる。よって未暗号化のデータをそのまま外部ネットワークに送出してしまう事態を回避できる。

【0212】また、本来、1（暗号化）の暗号化ビットが0に改ざんされた場合、署名情報がないと、次の暗号化装置で2回目の暗号化が行われてしまう。このケースは情報が外に洩れることはないが、受信先で正しく復号できないという事態を招く。しかし、このケースもデフォルト以外の署名情報が付いているのに暗号化ビットが0であるという矛盾を検出することでエラー処理に入ることができる。

【0213】以上のようなタイプ2のセキュリティゲートウェイの処理を図26に示す。

【0214】本セキュリティゲートウェイでは、データパケットを受け取ると（ステップS20）、まず、暗号化判定部16にて、暗号化ビットと署名情報を参照し、次のステップS21、S22、S23、S24の判断が行なわれる。

【0215】暗号化ビットが0で意味のある署名情報がついているか（ステップS21、S23）、暗号化ビットが1で意味のある署名情報がついていない場合（ステップS22、S24）は、エラー処理となる（ステップS30）。

【0216】暗号化ビットが0で意味のある署名情報がついていない場合（ステップS21、S23）、データ本体（24）を暗号化して（ステップS25）、次段に転送する（ステップS29）。

【0217】暗号化ビットが1で意味のある署名情報がついている場合（ステップS22、S24）、受信先ホストアドレス（22）がホストアドレス管理部14内に登録されているか判定し（ステップS26）、登録されているときは（ステップS27）、データ本体（24）を復号化して（ステップS28）、次段に転送し（ステップS29）、一方、登録されていないときは（ステップS27）、何も処理をせずに、次段に転送する（ステップS29）。

【0218】ただし、この場合、暗号化ビットを1から0に変え、かつ、署名情報を取り去ってしまうような改ざんを受けてしまうと適当なエラー検出はできない。そのため、そのように改ざんされたデータをセキュリティゲートウェイが受けとると、そのデータに2度目の暗号化処理を施してしまうことになる。この場合、受け手が

正しくデータ内容を得られない不具合が生じるが、データ内容の漏洩は起らない。

【0219】（タイプ3、タイプ4）次に、タイプ3、タイプ4のセキュリティゲートウェイについて説明する。

【0220】上記のタイプ1およびタイプ2のセキュリティゲートウェイの動作例では、図24に示すように、転送されるデータが送信元、受信先の小組織のみの秘密情報であり、経路途中のいかなる他の部署（たとえ上位階層の部署であっても）にも開示されないことを保証するものであった。

【0221】しかし、一般にネットワークを介して通信を行う場合、よりネットワークの外側でデータの暗号化、復号化を行いたい場合がある。

【0222】ここでは、一例として、図27に示すようなネットワークにおいて、マルチキャスト通信で複数の受信先にデータを通信する場合、具体的には、ホストxから自組織内の他部署のホストa、bと外部組織内のホストc、d、eにデータを転送する場合を考える。

【0223】この場合、自組織内では、送信元ホストから2つのセキュリティゲートウェイを通して接続されている部署a、bに同じデータを送信するので、暗号化はセキュリティゲートウェイA（送信元から3つめのセキュリティゲートウェイ）で行うようにすると、自組織内部署への送信は暗号化、復号化処理を行わずに高速に行うことができる。

【0224】また、外部組織側では、セキュリティゲートウェイB（受信先ホストから2つめのセキュリティゲートウェイ）で復号化を一度行えば、部署c、d、eの各々の入口のセキュリティゲートウェイでの復号化処理を回避でき、やはり転送効率を高めることが可能である。

【0225】この例における暗号化、復号化を行うセキュリティゲートウェイから送信元、受信先ホストへの経路数を暗号化、復号化レベルと定義し、所定の暗号化、復号化レベルのセキュリティゲートウェイで暗号化、復号化処理されることをユーザが指定する場合の構成、動作を考える。

【0226】まず、タイプ3のセキュリティゲートウェイについて説明する。

【0227】図28に、上記要求に応じるためのタイプ3のセキュリティゲートウェイの構成例である。図28の各構成部分の基本的な機能は、図21と同様である。

【0228】各データパケットには図29に示すようにデータ属性（図22中の23）内にそのデータパケットの発信者が要求する暗号化レベルおよび復号化レベルをコード化して与えておく。各セキュリティゲートウェイ内では、ホストアドレス管理部14内の管理情報に、そのセキュリティゲートウェイから下位にある全てのホストアドレスおよびそれらのホストに到達するレベル数を

記録しておく。例えば、図27のセキュリティゲートウェイAに含まれるセキュリティゲートウェイ内のホストアドレス管理部14には、図28に示すような情報が登録される。

【0229】本セキュリティゲートウェイでは、これらのデータパケット内に与えられた暗号化、復号化レベル要求およびホストアドレス管理部14内の情報を元に以下のように動作する。

【0230】本セキュリティゲートウェイは、データパケットの送信元ホストがホストアドレス管理部14に登録されており、かつ、そのホストのレベル数がデータパケット内に示された暗号化レベルに等しい場合に、暗号化部11でデータの暗号化を行う。また、受信先ホストがホストアドレス管理部14に登録されており、かつ、そのホストのネストレベルがデータパケット内に示された復号化レベルに等しい場合に、復号化部12でデータの復号化を行う。従って、図29に示す形式のデータパケットが図27のネットワーク構成でホストxから発信された場合、セキュリティゲートウェイAで暗号化され、セキュリティゲートウェイBで復号化されることになる。

【0231】次に、タイプ4のセキュリティゲートウェイについて説明する。

【0232】本セキュリティゲートウェイの構成は、図28のタイプ3のものと同様である。ただし、本セキュリティゲートウェイでは、データパケット内の暗号化、復号化レベルを1つの共通の情報で扱うと仮定し、1つのデータフィールドを共有して使用する。従って、ここでは、扱うデータパケットの形式は図30のようになる。

【0233】各セキュリティゲートウェイでは、送信元ホストがホストアドレス管理部14に登録されており、かつ、そのホストのレベル数がデータパケット内に示された暗号化、復号化レベルに等しい場合に暗号化部11でデータの暗号化を行う。また、受信先ホストがホストアドレス管理部14に登録されており、かつ、そのホストのレベル数がデータパケット内に示された暗号化、復号化レベルに等しい場合に復号化部12でデータの復号化を行う。

【0234】このタイプ3、タイプ4の2つの実施形態では、暗号化されていないデータがネットワークの複数のパスを通るので、タイプ1、2に比べセキュリティ的に劣ってしまうことが考えられる。また、データパケット内のデータについては、タイプ2で示した暗号化ビットの改ざんだけでなく、暗号化、復号化レベル情報も改ざんされる可能性があることを考慮しなくてはならない。これを防ぐには、タイプ2で説明したと同様の、暗号化を行ったセキュリティゲートウェイの署名機構、データのチェック機構を付加し、各ネットワーク経路上でデータの整合性をチェックし、もし矛盾のあるデータパ

ケットが入力された場合はエラー処理を行うようにすればよい。

【0235】一例として図31でホストxから暗号化レベル3でデータが送出され、このデータがセキュリティゲートウェイB、C間で改ざんされ、暗号化レベルが2に変えられてしまう場合を考える。この場合、セキュリティゲートウェイAで暗号化されるはずであったにもかかわらず、セキュリティゲートウェイAに到達するとホストxはレベル3であるから自装置では暗号化しない、と判断してしまい、暗号化されていないデータが外部に洩れていってしまうことになる。ここで、タイプ2の実施形態で説明したような暗号化ビットと暗号化署名情報を使い、セキュリティゲートウェイAで判定を行うと、そのような未暗号化情報の外部への漏洩が防止できる。すなわち、そのようなデータがセキュリティゲートウェイAに到達した場合、暗号化署名情報が元データのままであるから、ネットワークの下位では暗号化されていないことになり、暗号化レベルの情報と矛盾する。また、暗号化ビットも1になっていないので、その点でも矛盾がある。従ってセキュリティゲートウェイAはデータの内容が途中経路で改ざんされたと判定でき、エラー処理を行うことができる。

【0236】以上は、暗号化レベルが小さく改ざんされた場合であるが、暗号化レベルが大きく改ざんされる場合（エラー判定しないと、2重の暗号化がされてしまう）も同様に処理できる。

【0237】図32には、改ざんに対処できるタイプ3、タイプ4のセキュリティゲートウェイでの判定処理を示す。なお、ここでは、図25の暗号化判定部16の判定処理を最初に行なうものとしている。

【0238】本セキュリティゲートウェイでは、データパケットを受け取ると（ステップS40）、まず、暗号化判定部16にて、暗号化ビットと署名情報を参照し、次のステップS41、S42、S43、S46の判断が行なわれる。

【0239】暗号化ビットが0で意味のある署名情報がついているか（ステップS41、S43）、暗号化ビットが1で意味のある署名情報がついていない場合（ステップS42、S46）は、エラー処理となる（ステップS50）。

【0240】暗号化ビットが0で意味のある署名情報がついていない場合（ステップS41、S43）、データの暗号化レベルが登録された送信ホストのレベル数と同じならば（ステップS44）、ここで暗号化し（ステップS47）、データの暗号化レベルが登録された送信ホストのレベル数より大きいならば（ステップS45）、上位で暗号化し（ステップS48）、データの暗号化レベルが登録された送信ホストのレベル数より小さいならば、エラー処理となる（ステップS50）。

【0241】暗号化ビットが1で意味のある署名情報が

っている場合(ステップS42、S46)、既に暗号化完了と判断する(ステップS49)。

【0242】なお、ステップ47のようにここで暗号化すると判定された場合、暗号化した後に次段に転送する。また、ステップ48のように上位で暗号化すると判定された場合、またはステップ49のように既に暗号化完了と判定された場合、何も処理せずに次段に転送する。

【0243】本実施形態では、暗号化ビットの改ざんについてはタイプ2のセキュリティゲートウェイの場合と同様に処理することができる。

【0244】ここで、暗号化、復号化レベル情報や暗号化ビットなどの制御情報に、データ本体(24)とは別の暗号化を行い、実際に暗号化、復号化を行うセキュリティゲートウェイのみがこれらの情報を復号化できるようにして、よりセキュリティを高めることも可能である。

【0245】なお、タイプ3、4の実施形態における暗号化鍵の配布については、転送経路の全てのノード間で暗号化鍵を予め交換しておく方法や、転送要求が発生した際にデータ転送の前に送信元と受信先の間で鍵の交換を行うなどの方法が考えられるが、適当な方法を選択して行うものと仮定する。

【0246】さらに、本実施形態では、パケット暗号処理機能はセキュリティゲートウェイに一体化されているが、送信ホストもしくは受信ホストにもパケット暗号処理機能を内蔵することも可能である。特に、移動計算機を用いるモバイル・コンピューティング環境で必要となる。例えば、図1におけるホストH4が外部ネットに移動し、ホストH5の位置に移動したものとす。外部ネットはセキュリティゲートウェイで保護されていないため、送信パケットの暗号化および受信パケットの復号を移動ホスト自身が行う必要がある。

【0247】パケット暗号処理機能を送受信ホストに搭載した一構成例としては、図17において認証コード検査部(1611)をパケット復号部に、認証鍵管理部(1613)を暗号鍵管理部に、認証コード生成部(1614)をパケット暗号化部に、それぞれ置き換えたものとなる。

【0248】第1～第4の実施形態で説明した認証処理機能に係る発明と他の実施形態で説明した暗号処理機能に係る発明とは、独立実施可能である。すなわち、ゲートウェイにいずれかの認証処理機能およびいずれかの暗号処理機能の一方を設けてセキュリティゲートウェイとすることも、ゲートウェイにいずれかの認証処理機能およびいずれかの暗号処理機能の両方を設けてセキュリティゲートウェイとすることも可能である。

【0249】また、本実施形態では、全ゲートウェイに認証処理機能および/または暗号処理機能を設けてセキュリティゲートウェイとしているが、本発明を適用する

ネットワークに応じて、認証処理機能および/または暗号処理機能を設けないセキュリティゲートウェイが一部存在していても構わない。

【0250】また、本実施形態の各セキュリティゲートウェイの機能や計算機の機能は、プログラムとして実現することが可能である。

【0251】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0252】

【発明の効果】本発明によれば、送信元計算機を管理するパケット処理装置と受信先計算機を管理するパケット処理装置との間で認証手続きを行い、受信先計算機を管理するパケット処理装置は、認証法により受信したパケットの正当性を確認することができる。また、隣接するパケット処理装置間あるいは送信元計算機を管理するパケット処理装置と転送経路上の各パケット処理装置との間で認証手続きを行うことにより、各パケット装置はパケットの正当性を確認することができる。

【0253】特に、複数のパケット処理装置が正当性を確認可能であるため、保護ネットワークが階層化され、各階層にパケット処理装置を配置する場合においても、安全にパケット認証が行える。また、移動計算機を利用したモバイル・コンピューティング環境でも、移動ホストにパケット処理装置の機能を実装することにより安全にパケット認証を行うことができる。

【0254】また、本発明によれば、保護ネットワークが階層化され、各階層にパケット処理装置を配置する場合においても、重要な情報をネットワークを介して通信する際に、送信側でデータパケットを暗号化し、受信側で復号化する処理を、ユーザの指定する箇所でのみ行うことができ、暗号化、復号化の処理に起因するデータ転送効率の低下を防止することができる。さらに、そのようなネットワーク構成において、データに含まれる情報を共有すべき最小のネットワーク範囲を認識し、必要なネットワーク階層でのみ暗号化、復号化を行い、かつ不要な多段階の暗号化を回避するよう制御することが可能になる。

【0255】また、本発明によれば、各パケット処理装置で暗号化を行った際にデータパケットに暗号化完了を示す情報を付加し、この情報の付加されたデータパケットに対しては、その暗号化装置では暗号化を行わないように制御することができるので、各暗号化装置毎に複雑なネットワーク構成の設定を行うことなく、1回のみの暗号、復号化を行うようにシステムを設定することが可能になる。

【図面の簡単な説明】

【図1】本発明の実施の形態に係るセキュリティゲートウェイが用いられる計算機ネットワークの一構成例を示す図

【図2】図1の計算機ネットワークにおけるパケットの流れの一例を説明するための図

【図3】本発明の第1の実施形態に係るセキュリティゲートウェイの構成を示す図

【図4】パケットフォーマットの一例を示す図

【図5】パケット認証機能を実施するためのパケットフォーマットの一例を示す図

【図6】同本実施形態における認証鍵テーブルの一例を示す図

【図7】同本実施形態の動作を説明するための図

【図8】同本実施形態におけるセキュリティゲートウェイの処理手順を示すフローチャート

【図9】メッセージ認証子の多重化を効率化する方法におけるメッセージ認証子の計算対象データの一例を示す図

【図10】本発明の第2の実施形態に係る送信側のセキュリティゲートウェイの構成を示す図

【図11】同実施形態に係る転送経路上のセキュリティゲートウェイの構成を示す図

【図12】同実施形態の動作を説明するための図

【図13】同本実施形態における認証鍵テーブルの一例を示す図

【図14】同本実施形態におけるセキュリティゲートウェイの処理手順を示すフローチャート

【図15】本発明の第3の実施形態の動作を説明するための図

【図16】同実施形態におけるセキュリティゲートウェイの処理手順を示すフローチャート

【図17】同実施形態におけるセキュリティゲートウェイの処理手順を示すフローチャート

【図18】本発明の第4の実施形態の動作を説明するための図

【図19】パケット認証機構を送受信ホストに搭載した場合の構成を示す図

【図20】移動計算機を送信ホストとした場合のパケット認証機能の動作を説明するための図

【図21】本発明の他の実施形態に係るセキュリティゲートウェイ（タイプ1）の基本構成を示す図

【図22】同実施形態におけるデータパケットの一形式を示す図

【図23】同実施形態に係るセキュリティゲートウェイ（タイプ1）がデータパケットを受けとった際の動作手順を示すフローチャート

【図24】同実施形態に係るセキュリティゲートウェイにより実現される暗号化通信を示す概念図

【図25】データ属性に基づいて暗号化処理を行うセキュリティゲートウェイ（タイプ2）の基本構成を示す図

【図26】同実施形態に係るセキュリティゲートウェイ（タイプ2）がデータパケットを受けとった際の動作手順を示すフローチャート

【図27】同実施形態に係るセキュリティゲートウェイによりマルチキャスト通信を行う際のネットワーク基本構成およびデータ転送形態の一例を示す図

【図28】ユーザが暗号化、復号化レベルを個別に指定するセキュリティゲートウェイ（タイプ3）の基本構成を示す図

【図29】同実施形態に係るセキュリティゲートウェイ（タイプ3）におけるデータパケットのデータ属性の一形式を示す図

【図30】同実施形態に係るセキュリティゲートウェイ（タイプ4）におけるデータパケットのデータ属性の一形式を示す図

【図31】暗号化レベル情報が改ざんされる場合を説明するための図

【図32】同実施形態に係るセキュリティゲートウェイ（タイプ3、タイプ4）で暗号化レベル情報の改ざんの有無を判定するための処理の流れを示すフローチャート

【符号の説明】

101…インターネット

102…組織Aネットワーク

103…組織Bネットワーク

104…組織Cネットワーク

105…組織Dネットワーク

301, 501, 601…パケット受信部

302, 604…認証コード検査部

303, 503, 603…認証鍵管理部

304, 506, 606…パケットフィルタリング部

305, 504…認証コード生成部

306, 505, 605…パケット整形部

307, 502, 602…パケット転送部

GA, GA1, GA11, GB, GB1, GC, GD,

310…セキュリティゲートウェイ

510…（送信元）セキュリティゲートウェイ

610…（転送経路上）セキュリティゲートウェイ

1501…送信元ホストアドレス

1502…受信先ホストアドレス

1503…コネクションID

1504…認証コード

1505…データ部

H, H1, H2, H3, H4…ホスト

2, 2a, 2b, 2t…セキュリティゲートウェイ

3, 3s, 3d, host a~host e, hos

t v~host x…ホスト

11…暗号化部

12…復号化部

13…暗号鍵記憶部

14…ホストアドレス管理部

15…ホストアドレス比較部

16…暗号化判定部

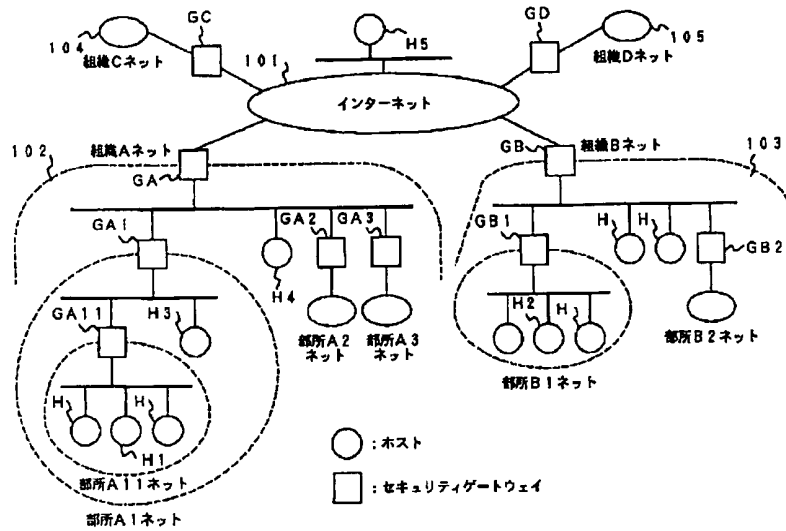
21…送信元ホストアドレス

22…受信先ホストアドレス

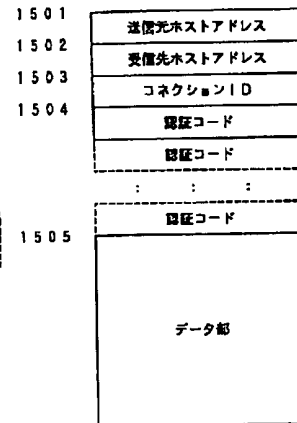
24…データ本体

23…データ属性

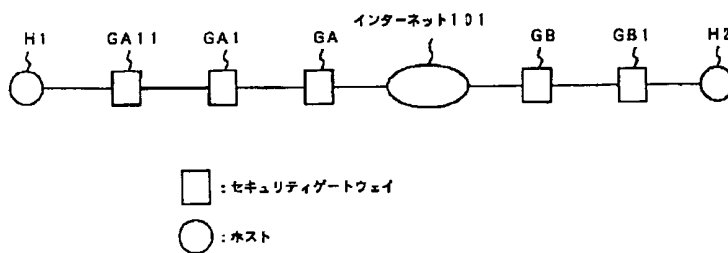
【図1】



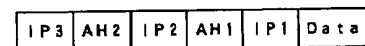
【図4】



【図2】



【図5】



【図6】

送信元ホスト アドレス	受信先ホスト アドレス	コネクション ID	検査用 認証値	証明用 認証値
H1	H2	ID1	K1	K2
H3	H2	ID1	...	K3, K4
H1	H4	ID2	K5	K6
H5	H3	ID3	K7, K8	...

【図9】



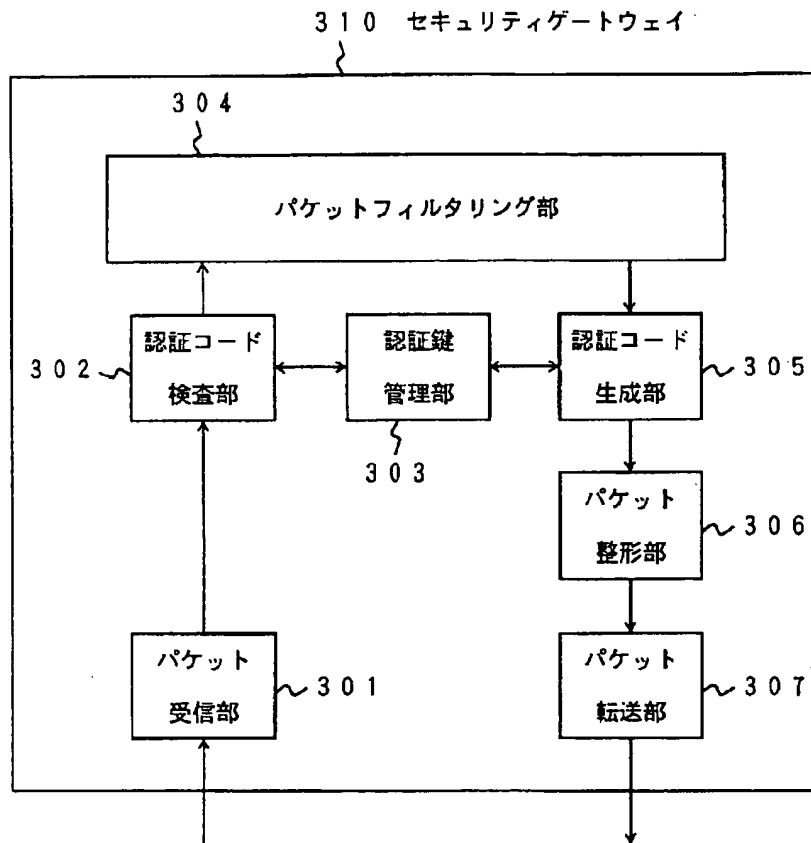
AH1内認証コードで保護

AH2内認証コードで保護

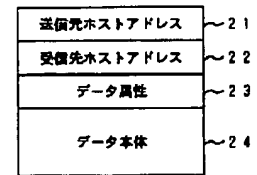
IP: IPヘッダ

AH: 認証ヘッダ

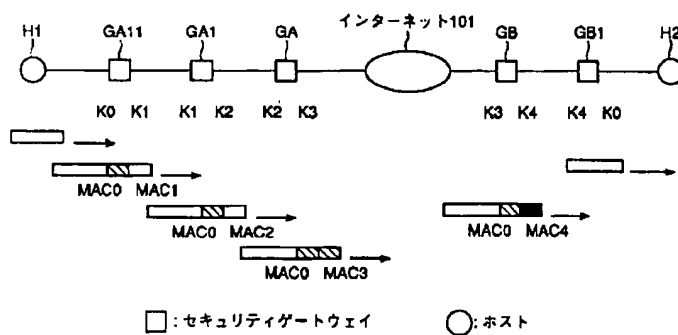
【図3】



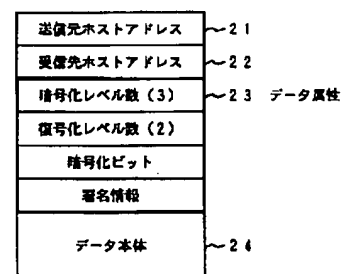
【図22】



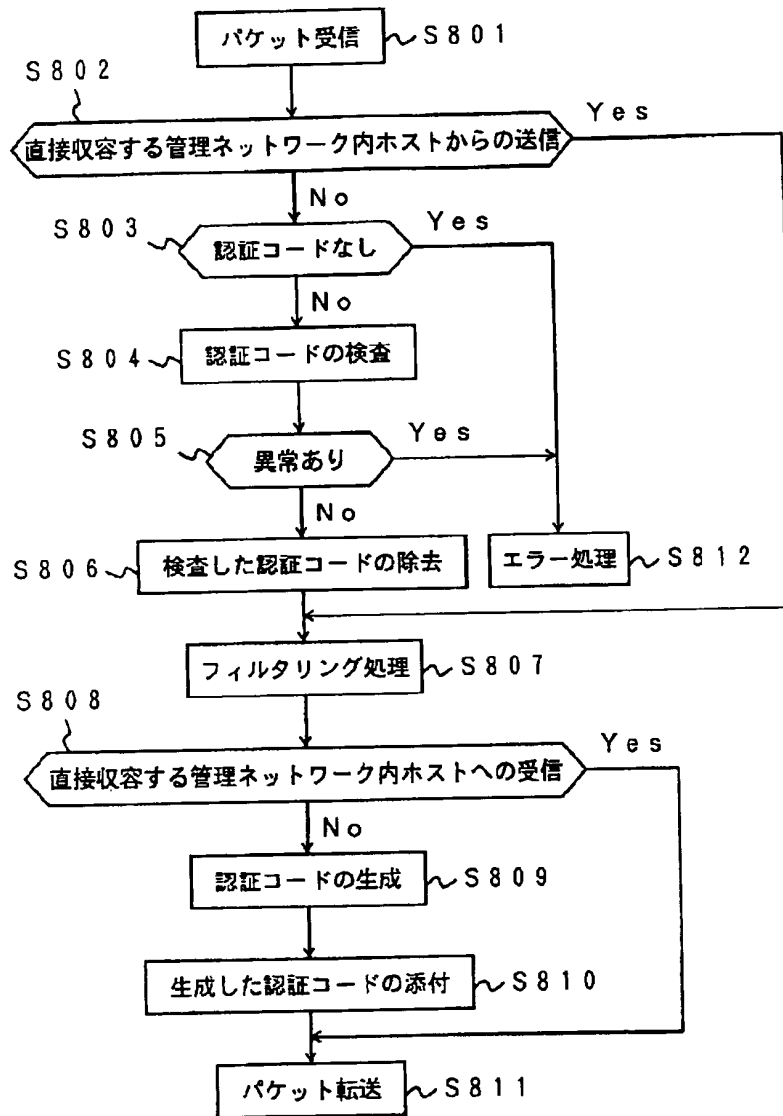
【図7】



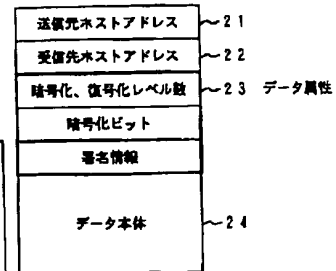
【図29】



【図8】



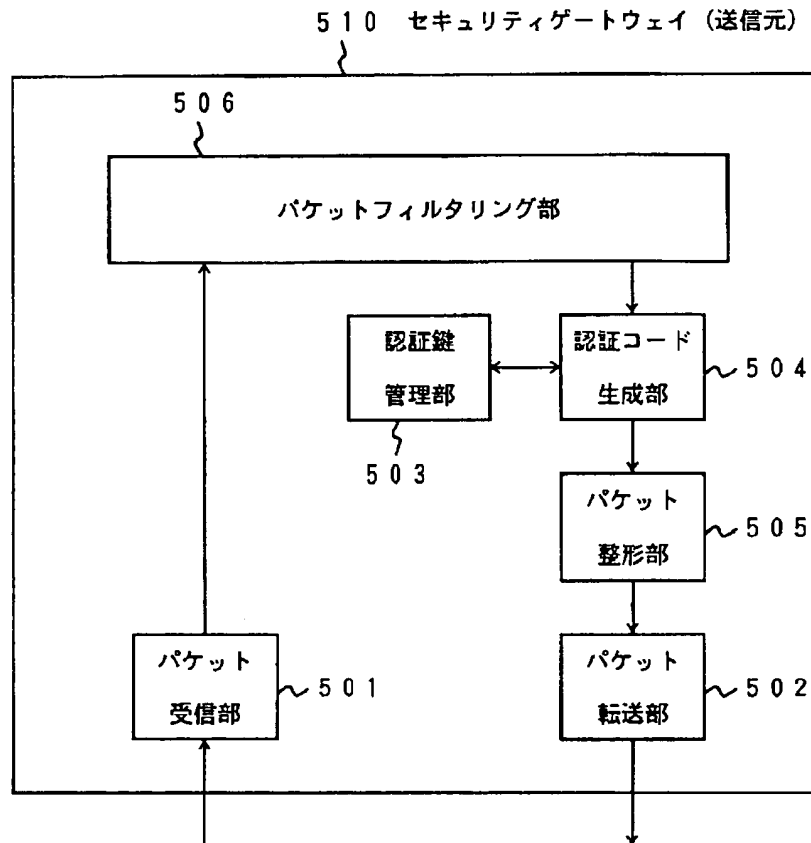
【図30】



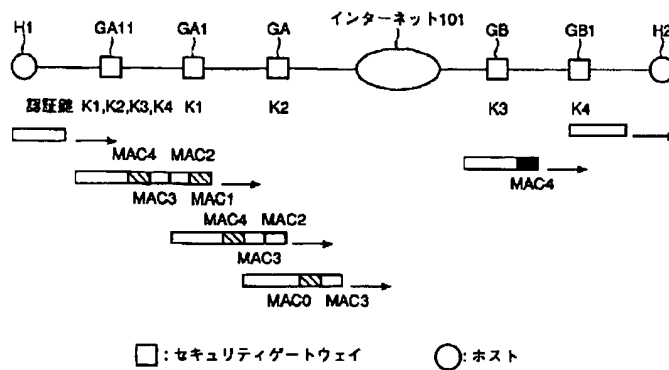
【図13】

送信元ホスト アドレス	受信先ホスト アドレス	コネクション ID	検査用 暗証鍵	証明用暗証鍵
H1	H2	ID1	K1	...
H3	H2	ID1	...	K2, K3, K4, K5
H1	H4	ID2	K6	...
H5	H3	ID3	K7	...

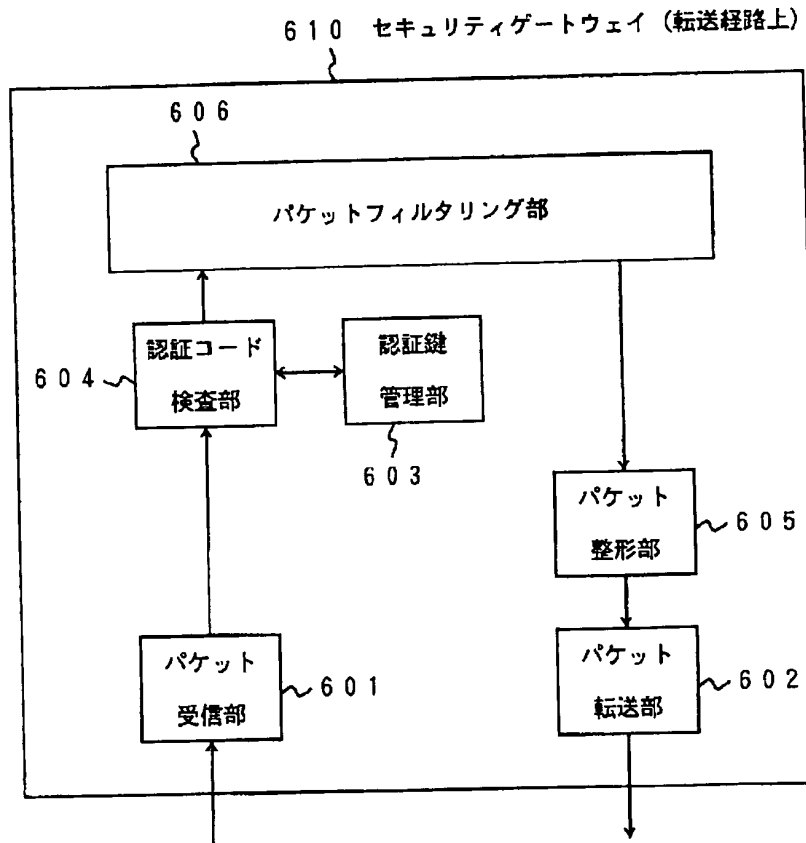
【図10】



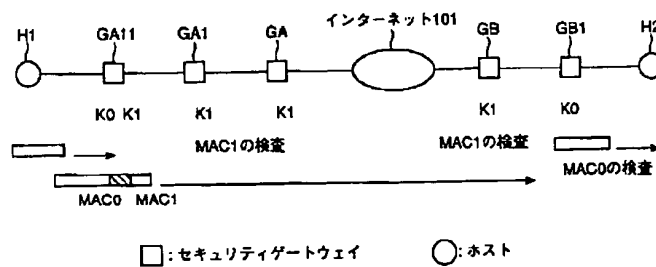
【図12】



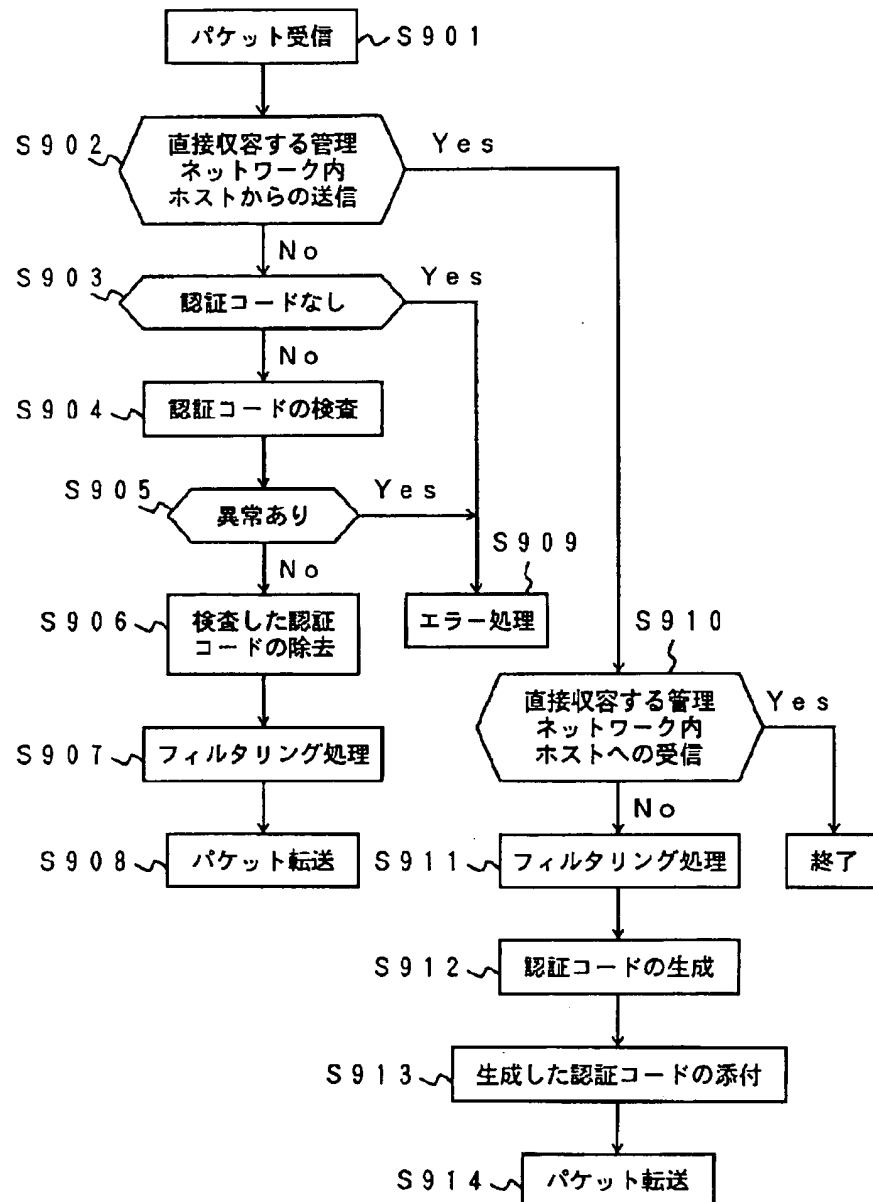
【図11】



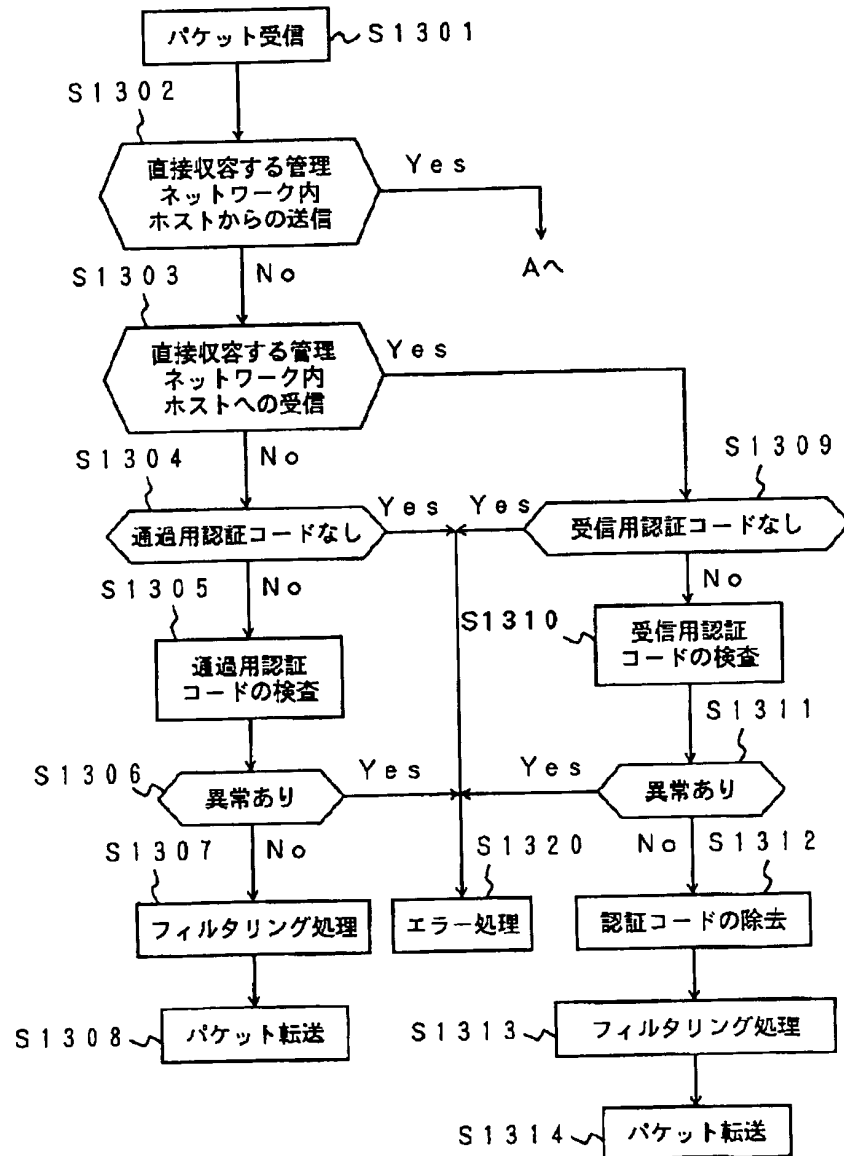
【図15】



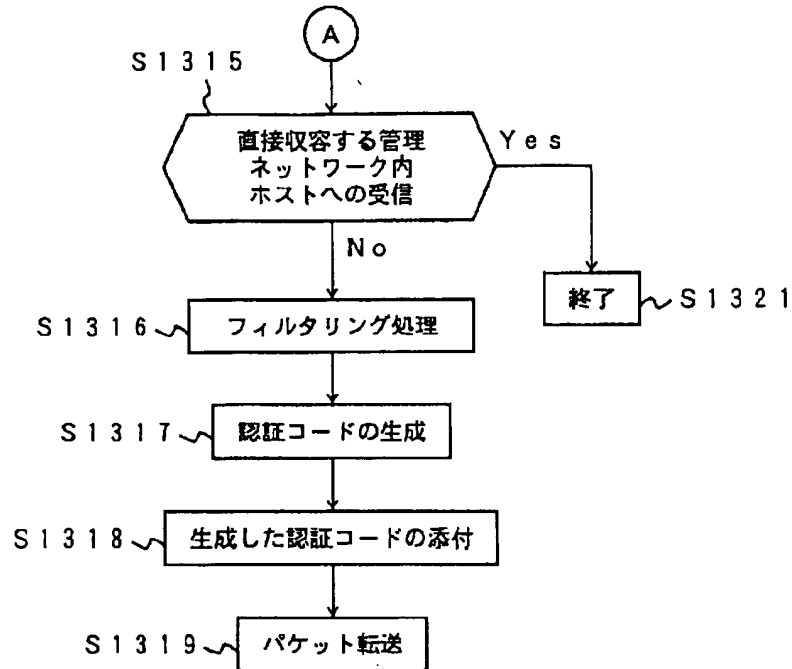
【図14】



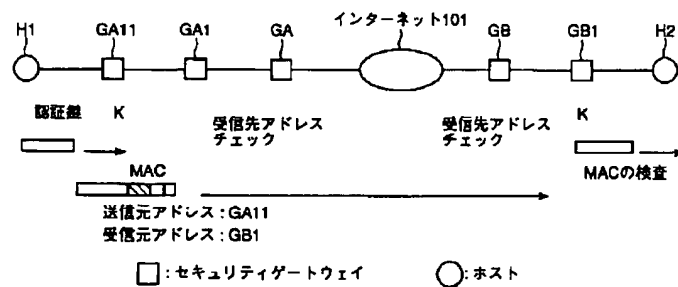
【図16】



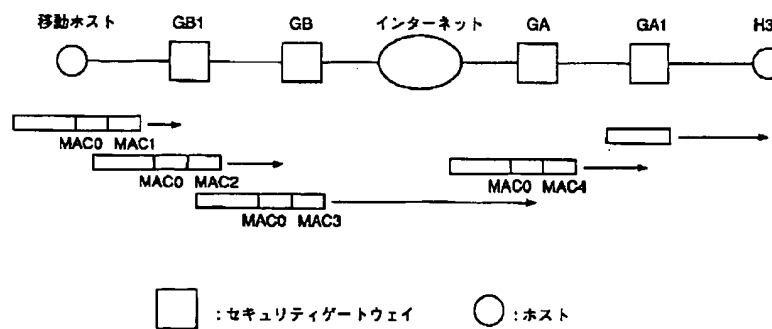
【図17】



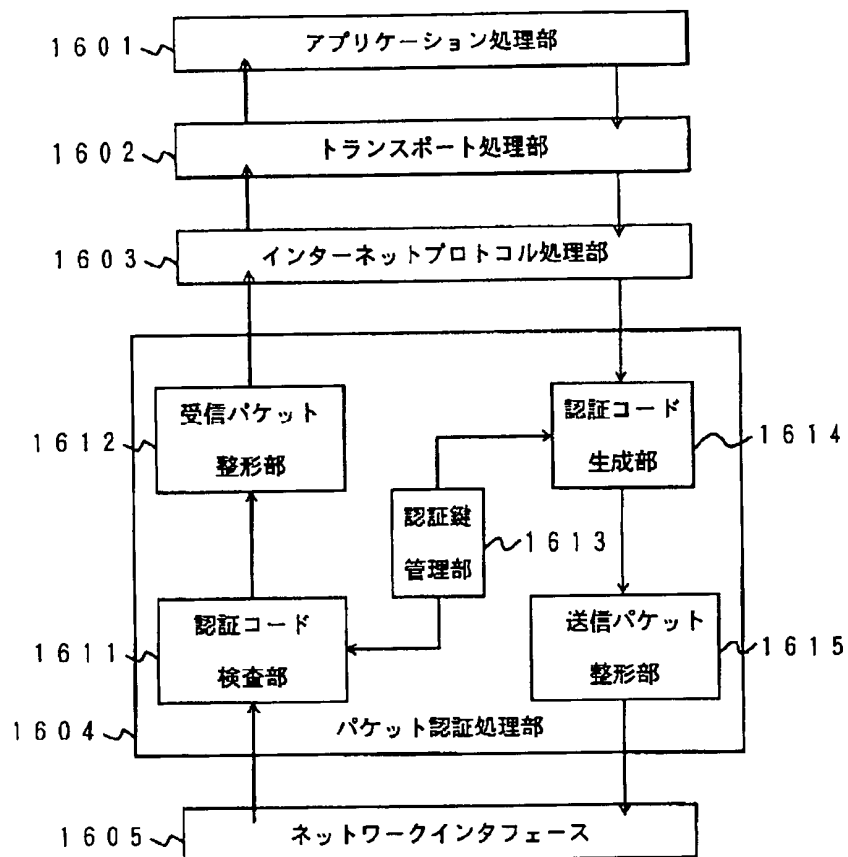
【図18】



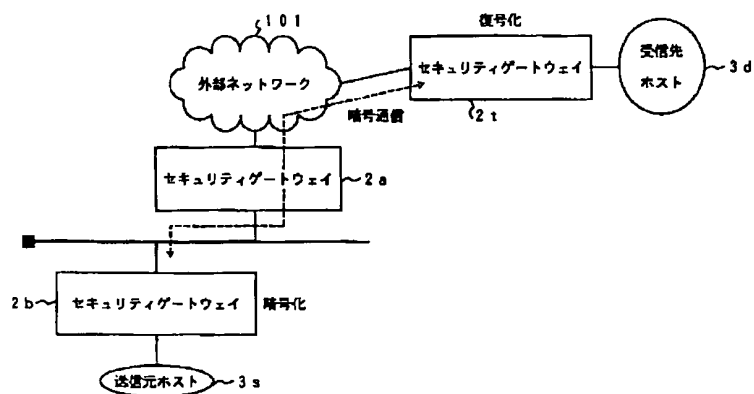
【図20】



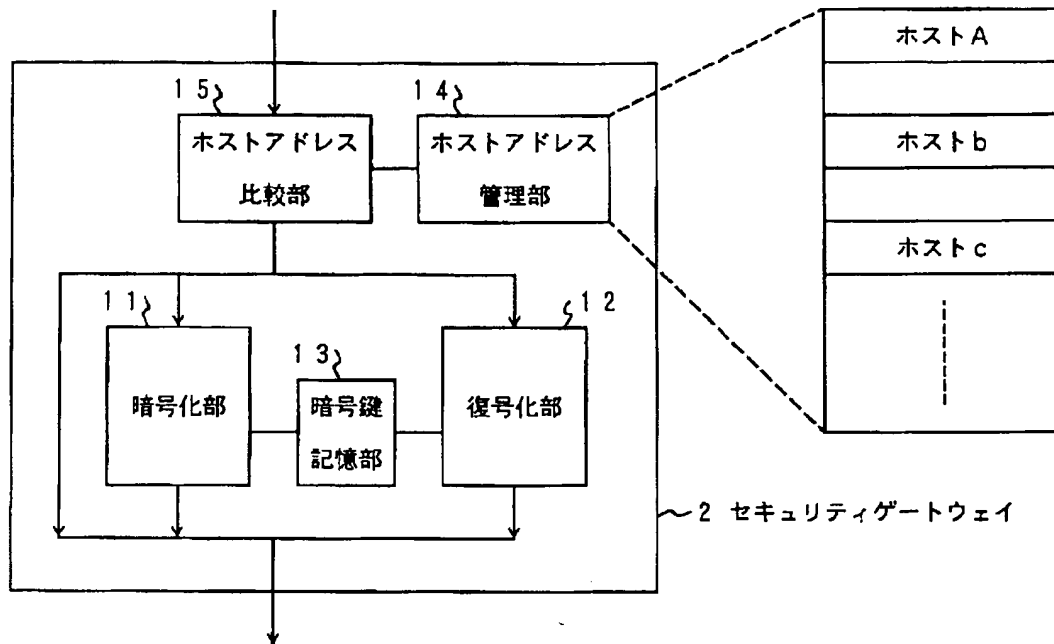
【図19】



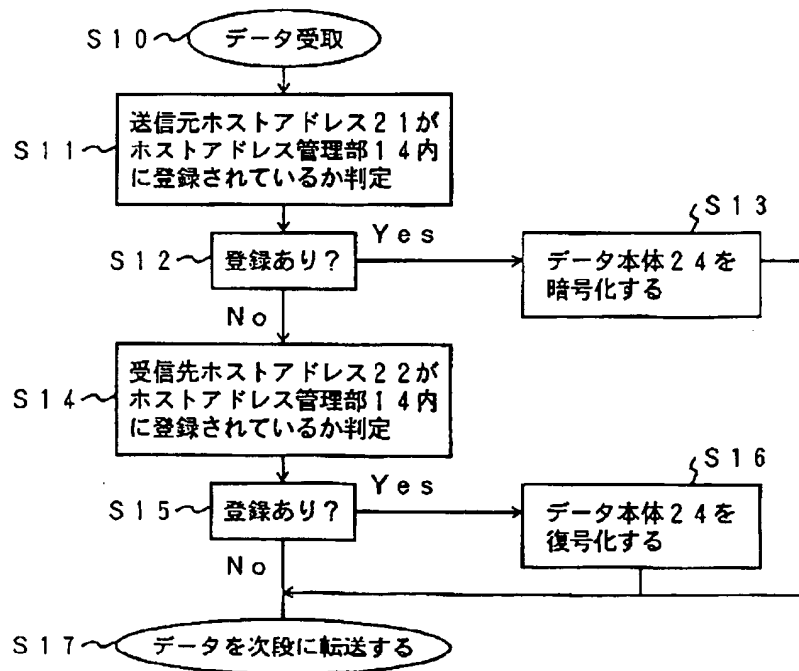
【図24】



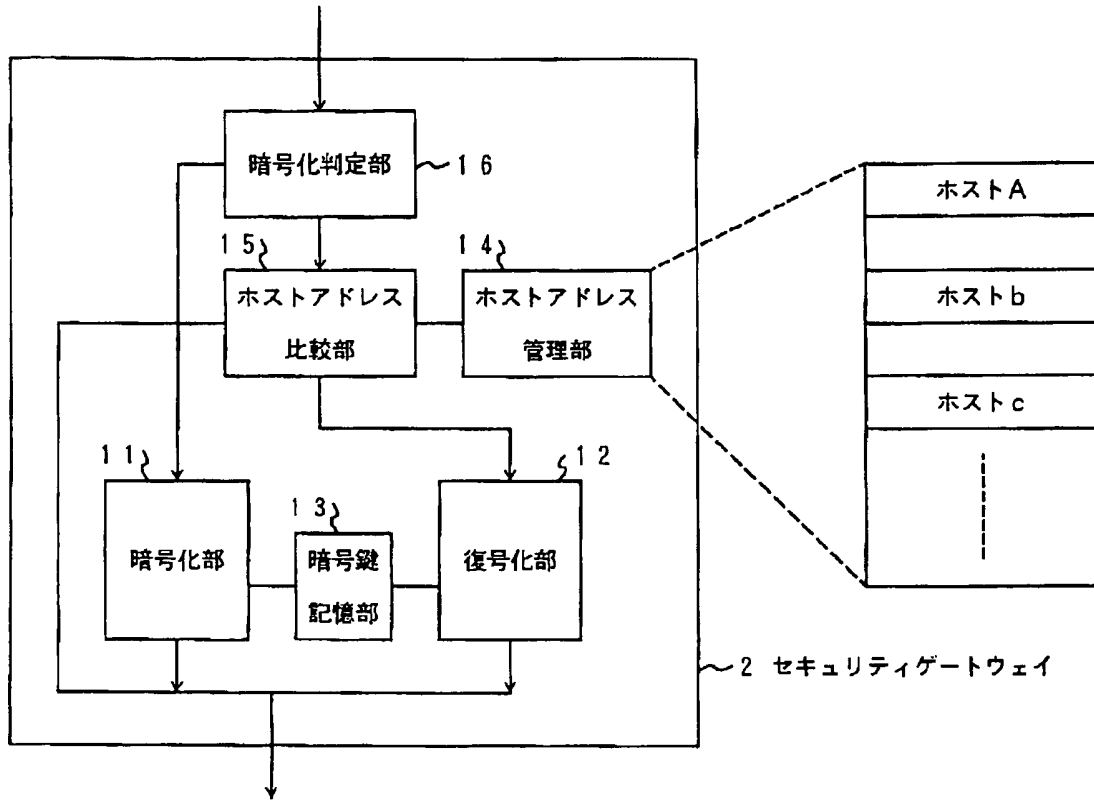
【図21】



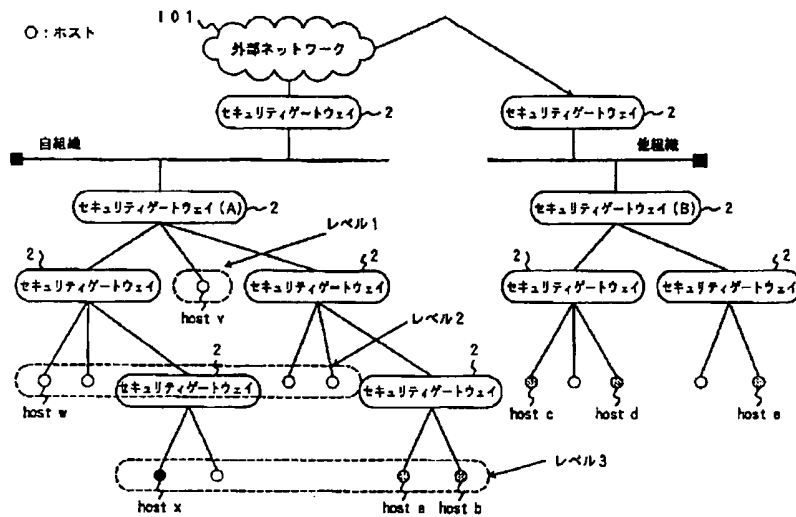
【図23】



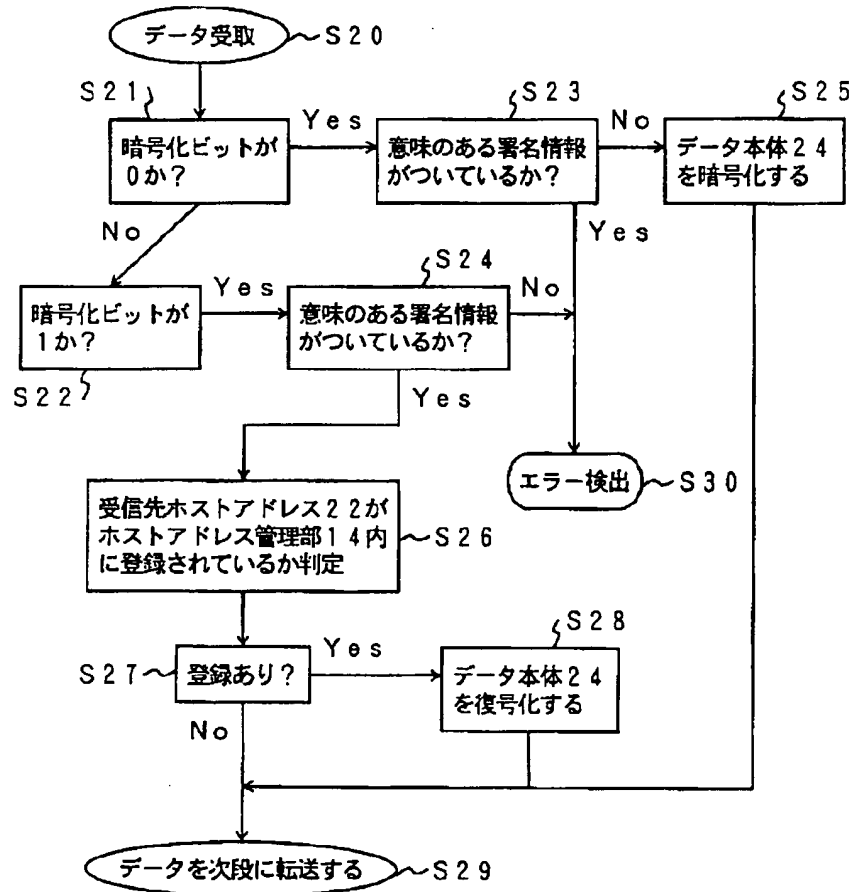
【図25】



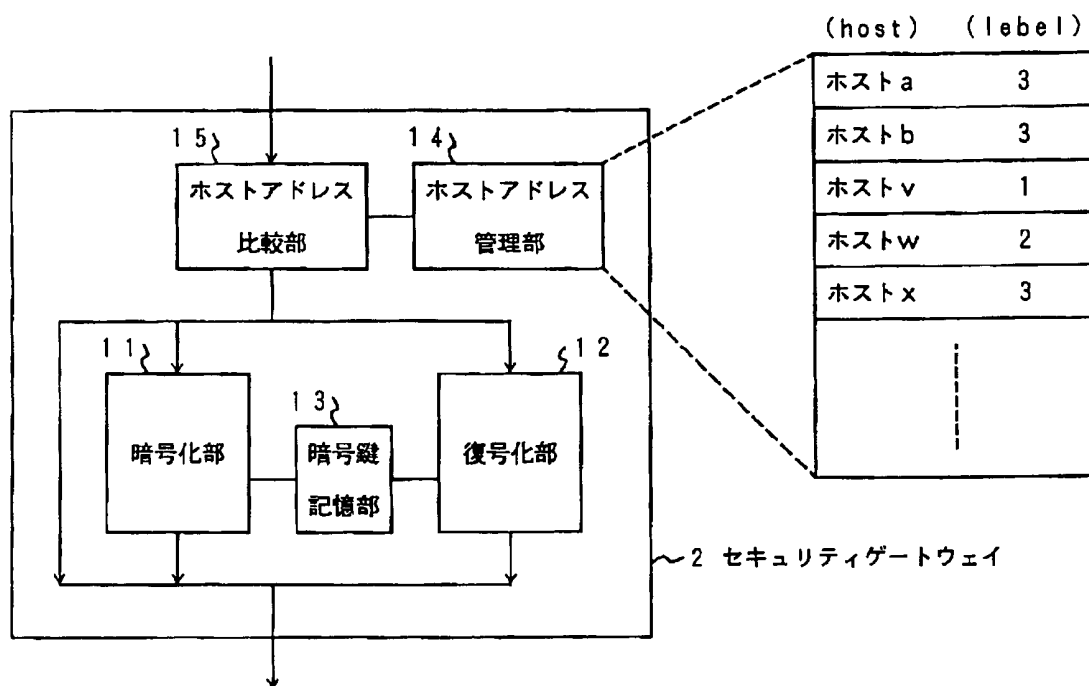
【図27】



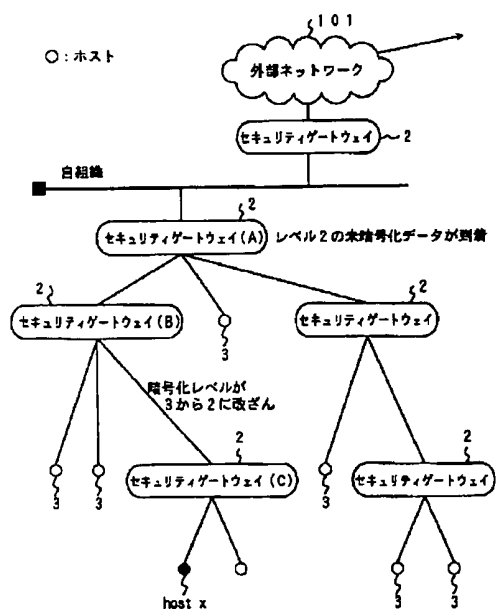
【図26】



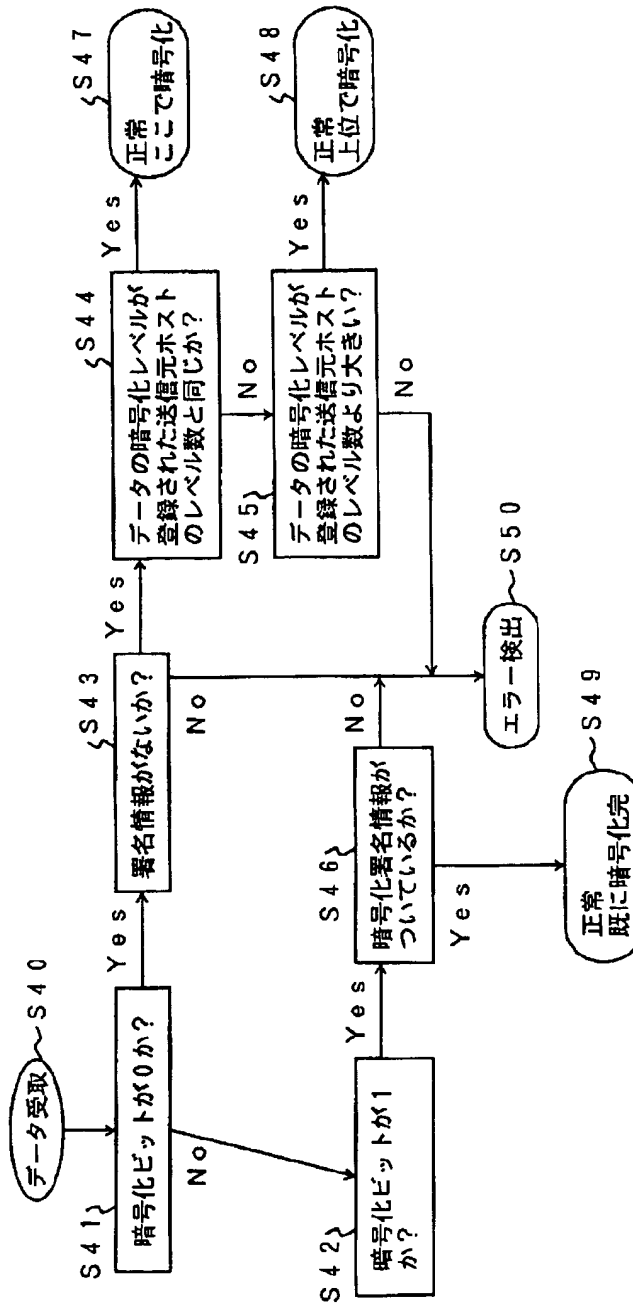
【図28】



【図31】



【図32】



フロントページの続き

(72)発明者 岡本 利夫
 神奈川県川崎市幸区小向東芝町1番地 株
 式会社東芝研究開発センター内

THIS PAGE BLANK (USPTO)